Haute école de Namur Liège Luxembourg

Implantation IESN – Sécurité des systèmes

Étude et implémentation de solutions pour l'analyse forensique en entreprise

Grégoire Roumache

Travail de fin d'études présenté en vue de l'obtention du diplôme de bachelier en sécurité des systèmes

Maître de stage
Arnaud Rosette

Promoteur
Christophe Debut

Année académique 2021-2022

Table des matières

Synopsis

"Chaque crime laisse une trace", ce principe a été énoncé par Edmond Locard, pionnier de la police scientifique à une époque où l'informatique n'existait pas. Et pourtant, il s'applique également à ce domaine parce que chaque acteur dans un système informatique laisse une trace de son passage. L'étude du comportement des acteurs malveillants sur un système et l'obtention des indicateurs de compromission (*Indicator of Compromise* ou *IoC* en anglais) est essentiel pour déterminer l'étendue d'une attaque informatique et y mettre fin.

L'objectif de ce travail est de participer à l'amélioration de la détection et de l'analyse des menaces dans l'entreprise. Pour arriver à cela, mon travail s'est focalisé sur la recherche d'un ensemble d'outils, la conception et l'implémentation d'une solution et des procédures d'acquisition et d'analyse forensique.

La première section de ce travail est consacrée à l'analyse comparative des outils. La combinaison de la recherche théorique et de l'expérimentation pratique ont permis de sélectionner les outils les plus appropriés sur base d'une liste de besoins.

La deuxième section de ce travail se concentre sur la conception et l'implémentation d'une solution. Son architecture a été conçue pour prévenir la propagation des menaces afin de pouvoir l'utiliser sans augmenter les risques pour l'entreprise. Elle comporte notamment une sandbox pour analyser des logiciels malveillants mais aussi des outils d'analyse de la mémoire volatile et non-volatile permettant de montrer la présence, l'exécution et l'origine d'un logiciel malveillant.

La troisième section de ce travail est dédiée aux procédures. Elles ont été travaillées en se basant sur celles utilisées par des institutions privées comme publiques tout en les adaptant au contexte de l'entreprise.

Enfin, des pistes d'amélioration sont envisagées et notamment après avoir utilisé cette solution dans des cas réels.

Bibliographie

[1] *Générateur gratuit de sources au format APA*. (2022, 23 mai). Scribbr. Consulté le 29 mai 2022, à l'adresse `https://www.scribbr.fr/generateur-apa/`