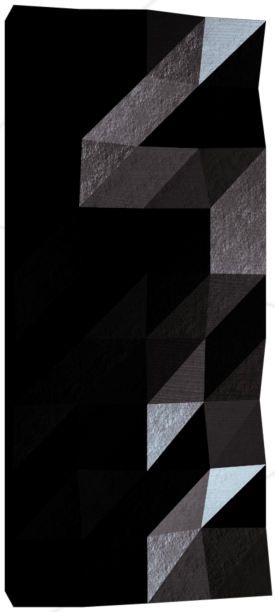

Bootcamp Cybersecurité | 42

recovery

Résumé: Collecte d'éléments de preuve

Version: 1

Table des matières

Chapitre I

Prologue

"social engineering" — la manipulation occasionnelle ou calculée des gens pour les influencer à faire des choses qu'ils ne feraient pas normalement. Et les convaincre sans sans éveiller le moindre soupçon.

Source : https://en.wikipedia.org/wiki/Kevin_Mitnick

Chapitre II

Introduction

La collecte de preuves est un processus essentiel qui doit être effectué avant de réaliser tout type d'analyse médico-légale. Avoir des preuves claires et organisées va facilitera votre travail. L'objectif de ce projet est de faire un programme qui capable d'extraire certains artefacts sur un laps de temps donné :

Chapitre III

Instructions générales

Vous travaillerez toujours sur une VM Win10. Vous pouvez utiliser une machine Vagrant par exemple : cette machine. Vous êtes autorisé à utiliser n'importe quel langage de programmation. Dans le cas où vous décidez d'utiliser un langage compilé, vous devrez remettre votre code source qui sera compilé lors de l'évaluation. compilé pendant l'évaluation.

Vous êtes autorisé à utiliser toute bibliothèque qui vous aide à développer cet outil, cependant vous devez être capable de justifier pourquoi vous les utilisez pendant l'évaluation.

Chapitre IV

Partie obligatoire

Vous devrez développer un programme qui extrait les artefacts suivants sur un un laps de temps donné :

- Date de modification des branches du registre (CurrentVersionRun)
- Fichiers récemment utilisés/ouverts
- Programmes installés
- Processus d'exécution
- Historique du navigateur Web
- Appareils connectés
- Journaux d'événements

Si l'utilisateur ne donne pas de plage de temps à votre programme, il doit se rabattre sur une valeur par défaut, par exemple : dernières 24h, dernière semaine, dernier mois...

Chapitre V

Partie bonus

L'évaluation des bonus se fera `SI ET SEULEMENT SI` la partie obligatoire est `PARFAITE`. Dans le cas contraire, les bonus seront totalement `IGNORÉES`.

Vous pouvez améliorer votre projet grâce aux fonctionnalités suivantes :

- Composez une ligne du temps où toutes les preuves sont affichées, organisées par catégories et par temps.
- Afficher l'arborescence du répertoire sur une sorte de vue graphique.

Chapitre VI

Évaluations peer 2 peer

Ce projet sera corrigé par d'autres étudiants. Remettez les fichiers dans le dépôt Git et assurez-vous que tout fonctionne comme prévu.