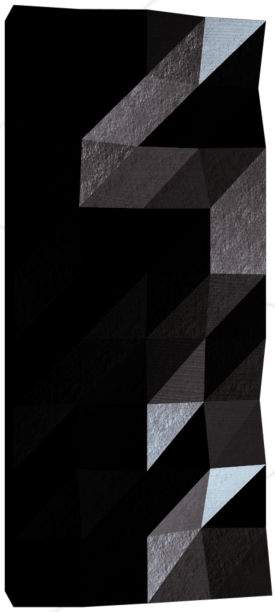

Bootcamp Cybersecurité | 42

extraction

Résumé: Récupération de fichiers supprimés sur le système de fichiers NTFS

Version: 1

Table des matières

Chapitre I

Prologue

Le seul système qui soit vraiment sûr est celui qui est éteint et débranché, enfermé dans un coffre-fort en titane, enterré dans un bunker en béton, et qui est entouré de gaz neurotoxiques et de gardes armés très bien payés. Même dans ce cas, je ne parierais pas ma vie dessus.

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

Chapitre II

Introduction

Dans ce projet, vous vous familiariserez avec le MFT (Master File Table) du système de fichiers NTFS (New Technology filesystem). L'objectif de ce projet est de développer un outil capable de récupérer des fichiers supprimés sur NTFS. Comme nous le savons tous dans la plupart des systèmes de fichiers, lorsque vous supprimez un fichier, il n'est pas vraiment supprimé, il reste là à moins d'être écrasé, pour cette raison, dans de nombreux cas vous serez être en mesure de récupérer des fichiers supprimés lors de l'exécution d'une analyse forensic.

Chapitre III

Instructions générales

Vous travaillerez toujours sur une VM Win10. Vous pouvez utiliser une machine Vagrant par ex celle ci. Vous êtes autorisé à utiliser n'importe quel langage de programmation. Si 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 devez développer un programme qui récupère les fichiers récemment supprimés. Pour cela votre programme devra être capable de faire les choses suivantes :

- Vous allez effectuer une recherche sur le disque entier.
- Vous verrez une liste de tous les fichiers récupérés.
- Vous montrerez si le fichier peut être complètement récupéré, seulement partiellement ou s'il a été trouvé mais n'est pas récupérable.
- S'il y a des fichiers disponibles pour la récupération, l'utilisateur pourra sélectionner ceux qu'il veut récupérer.

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

Les évaluations bonus ne seront effectuées que si votre partie obligatoire est `PARFAITE`. Sinon, les bonus seront IGNORÉES.

Vous pouvez améliorer votre projet grâce aux fonctionnalités suivantes :

- L'utilisateur peut sélectionner un répertoire et effectuer la recherche à partir de ce point au lieu de parcourir l'ensemble du disque.

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.