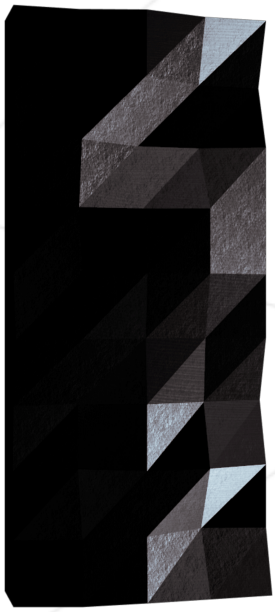

Bootcamp Cybersecurité | 42

Iron Dome

Résumé: Mieux vaut prévenir que guérir.

Version: 1

Table des matières

I	**Introduction**	**2**
II	**Partie obligatoire**	**3**
III	**Partie bonus**	**4**
IV	**Évaluations peer 2 peer**	**5**

Chapitre I

Introduction

Ceci est la deuxième partie de la branche ransomware. Dans cette partie, vous allez développer un outil spécifique qui va détecter une activité anormale en surveillant différents paramètres du système d'exploitation.

Malheureusement, il n'existe pas de moyen totalement efficace pour prévenir les attaques de ransomware, mais après avoir terminé ce projet, vous serez en mesure de comprendre les points faibles d'un système informatique en ce qui concerne ces infections par des logiciels malveillants.

Chapitre II

Partie obligatoire

Vous allez créer un programme appelé `irondome` qui répond aux spécifications suivantes.

- Il sera développé pour la plateforme Linux.
- Le programme ne s'exécutera que s'il est lancé en tant que root.
- Le programme fonctionnera en arrière-plan comme un démon ou un service.
- Le programme surveillera une zone critique à perpétuité. Ce parcours doit être indiqué comme un argument.
- Si plus d'un argument est fourni, ceux-ci correspondront aux extensions de fichiers à observer. Sinon, tous les fichiers seront surveillés.
- Le programme détectera les abus de lecture de disque.
- Le programme détectera l'utilisation intensive de l'activité cryptographique.
- Le programme détectera les changements dans l'entropie des fichiers.
- Le programme ne devrait jamais dépasser 100 Mo de mémoire utilisée.

Toutes les alertes doivent être signalées dans le fichier `/var/log/irondome/irondome.log`.

Chapitre III

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 :

- Le programme crée un dossier `backup` dans le répertoire HOME de l'utilisateur et effectue des sauvegardes incrémentielles à des intervalles configurables.

Chapitre IV

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.