

Gestion des incidents de sécurité : Forensics informatique



Introduction

Salut à tous ! Lorsqu'une faille de sécurité est exploitée ou qu'une attaque informatique a lieu, comment pouvons-nous déterminer ce qui s'est passé ? Comment retracer les étapes de l'attaquant ? La réponse réside dans le domaine fascinant de la "forensics informatique". Aujourd'hui, nous plongerons dans cet univers pour comprendre ses fondamentaux.

1. Qu'est-ce que la forensics informatique ?

La forensics informatique est l'art et la science de collecter, préserver, analyser et présenter des preuves numériques dans le but de découvrir ce qui s'est passé lors d'un incident de sécurité, d'identifier les coupables et, éventuellement, de les poursuivre en justice.

2. Les étapes clés de la forensics informatique

- **Identification :**
- La première étape consiste à identifier où se trouvent les preuves potentielles. Cela pourrait être un serveur compromis, un ordinateur personnel ou même un smartphone.
- **Préservation :**
- Une fois les preuves identifiées, il est crucial de les préserver dans leur état actuel. Cela signifie créer une image disque, qui est une copie exacte du disque dur, pour éviter toute altération des données.
- **Analyse :**
- Lors de cette phase, les experts utilisent divers outils et techniques pour examiner l'image disque. Ils cherchent des indices sur la manière dont l'attaque a été menée et sur l'identité de l'attaquant.
- **Documentation :**
- Toutes les découvertes doivent être soigneusement documentées. Cela comprend la prise de notes, la capture d'écrans et la création de rapports détaillés.
- **e. Présentation :**
- Les résultats de l'analyse sont ensuite présentés aux parties concernées, qui peuvent être des responsables d'entreprise, des forces de l'ordre ou un tribunal.

3. Exemple concret

Imaginons une entreprise qui a été victime d'une attaque par ransomware. L'attaquant a crypté des fichiers essentiels et demande une rançon. La forensics informatique serait utilisée pour :

- Identifier l'origine de l'attaque (par exemple, un email de phishing).
- Préserver l'état actuel des systèmes pour l'analyse.
- Analyser comment le ransomware s'est propagé dans le réseau.
- Documenter chaque étape de l'attaque.

4. Outils courants en forensics informatique

Il existe de nombreux outils spécialisés pour aider les experts en forensics. Voici quelques-uns des plus populaires :

Autopsy : Un outil d'analyse de disque dur open source.

Wireshark : Un analyseur de paquets pour étudier le trafic réseau.

Volatility : Un outil d'analyse de la mémoire pour extraire des informations d'une image de la mémoire.

Je retiens



La forensics informatique est un processus de collecte et d'analyse de preuves numériques après un incident de sécurité.



Les étapes clés comprennent l'identification, la préservation, l'analyse, la documentation et la présentation des preuves.



De nombreux outils sont disponibles pour aider dans ce processus, chacun ayant ses propres spécialités et utilisations.



La forensics informatique est essentielle pour comprendre les attaques, responsabiliser les coupables et renforcer la sécurité à l'avenir.

