Khar9ana Academy

Analyser des journaux de connexion

Lire un événement, reconstituer une chronologie, séparer les faits des hypothèses.

1. Lire un événement
2. Reconstituer une chronologie
3. Séparer faits et hypothèses
4. Rendre compte

Forensics, niveau débutant · Français · Édition de novembre 2026

Support original Khar9ana. Les comptes, les événements et les adresses sont fictifs.

1. Lire un événement

Un journal de connexion garde une trace de chaque tentative d'accès. Chaque ligne est un événement. Avant de l'interpréter, posez-lui quatre questions.

Question	Champ	Exemple fictif
Quand ?	Horodatage et fuseau	09:41 UTC
Qui ?	Compte visé	samir
D'où ?	Adresse source	192.0.2.14
Et alors ?	Résultat	échec

Le journal prouve qu'une tentative a utilisé un nom de compte. Il ne prouve pas qui était devant le clavier.

2. Reconstituer une chronologie

Ramenez les heures dans un même fuseau, triez du plus ancien au plus récent, regroupez par compte, puis repérez les changements de résultat.

```
09:41  samir  échec   192.0.2.14
09:42  amira  réussi  192.0.2.30
09:43  samir  échec   192.0.2.14
09:44  samir  échec   192.0.2.14
09:45  samir  réussi  192.0.2.14
```

La connexion d'amira s'intercale dans le temps, mais elle n'appartient pas à la séquence de samir.

3. Séparer faits et hypothèses

« Trois échecs précèdent une réussite » est un fait : chacun peut le relire dans le journal. « Le compte est compromis » est une hypothèse. Une personne qui se trompe de mot de passe produit la même trace.

Pour chaque hypothèse, cherchez l'information qui pourrait la contredire : une confirmation du titulaire, une adresse habituelle, l'activité qui suit la connexion.

4. Rendre compte

Constat. Entre 09:41 et 09:45 UTC, le compte samir connaît trois échecs puis une réussite depuis 192.0.2.14.

Limite. Ces lignes ne permettent pas d'identifier la personne.

Suite. Confirmer l'activité avec le titulaire et examiner ce qui suit 09:45.

Fiche de méthode

1. Fuseau de référence et période examinée

2. Compte et sources observées

3. Séquence retenue, dans l'ordre

4. Faits établis

5. Hypothèse, et ce qui pourrait la contredire

6. Vérification suivante

Pour pratiquer : rubrique Labs de Khar9ana, puis les défis de la catégorie Forensics.