Projet Sécurité: CTF

GROUPE	BACKDOOR	**SCENARIO 21/10**
PHASE 1	DEVELOPPEMENT CTF	***Réseaux***
NIVEAU	MOYEN	

La Fuite de Données Sensibles

Contexte: Vous travaillez en tant qu'analyste de sécurité pour l'entreprise XYZ. Cette entreprise détient des données sensibles sur ses clients et ses produits. Récemment, il y a eu une fuite de données confidentielles, et l'entreprise est déterminée à découvrir qui est responsable de cette fuite.

Objectif : Identifier l'employé qui a divulgué des données confidentielles de l'entreprise.

Niveau 1 - Analyse des Accès au Système :

- **Défi 1 : Examen des Logs d'Authentification**
  - Contexte : Vous commencez l'enquête en examinant les logs d'authentification du système. Vous découvrez un nom d'utilisateur suspect ayant des activités d'authentification anormales. Votre objectif est de trouver ce nom d'utilisateur suspect, qui pourrait être lié à la fuite de données.

Niveau 2 - Analyse des Activités sur les Serveurs :

- **Défi 2 : Identification des Accès Suspects**
  - **Contexte :** En utilisant le nom d'utilisateur suspect découvert au niveau 1, vous identifiez des activités serveur anormales, telles que des accès non autorisés à des dossiers sensibles, des tentatives de téléchargement de fichiers confidentiels, ou des modifications non autorisées. Votre objectif est de trouver des preuves dans ces activités serveur.

Niveau 3 - Examen des Communications Chiffrées :

- **Défi 3 : Déchiffrement des Communications Chiffrées**
  - **Contexte :** Vous avez identifié des activités suspectes liées à l'utilisateur suspect. Cependant, les données impliquées dans ces activités sont chiffrées pour protéger leur confidentialité. Dans ce défi, vous devrez déchiffrer ces communications chiffrées pour obtenir des informations essentielles sur la divulgation des données confidentielles, telles que le contenu des fichiers ou les détails des transmissions.

Niveau 4 - Identification de l'Employé Coupable :

- **Défi 4 : Enquête sur les E-mails Sortants**

Contexte : Vous avez collecté suffisamment d'informations pour identifier l'employé coupable de la fuite de données. Cependant, pour confirmer son identité, vous devez enquêter sur les e-mails sortants de cet employé. Vous cherchez un e-mail compromettant qui révèle son implication dans la fuite de données. Une fois que vous avez identifié l'employé coupable, votre objectif est atteint.