Projet : Analyse Forensique de Cyberattaque AFC

Profil : Cyber

Objectif du Projet : L'objectif principal de ce projet est de permettre aux étudiants de développer des compétences en analyse forensique en simulant une cyberattaque. Les étudiants auront pour tâche de mener une enquête approfondie pour comprendre la portée de l'attaque, identifier les acteurs impliqués, et proposer des mesures correctives.

Étapes du Projet :

1. **Préparation de l'Environnement :**
    - Créez un environnement virtuel simulant une infrastructure d'entreprise avec des serveurs, des postes de travail, des routeurs, etc.
    - Simulez une attaque en injectant des fichiers malveillants, en modifiant des configurations, ou en utilisant d'autres vecteurs d'attaque.
2. **Détection de l'Incident :**
    - Les étudiants devront mettre en place des outils de surveillance et de détection des incidents.
    - Enregistrez les journaux d'événements, les données réseau, les fichiers système, etc.
    - Les équipes de défense doivent être prêtes à détecter et à signaler l'incident.
3. **Isolation et Préservation des Preuves :**
    - Dès la détection de l'incident, l'équipe doit isoler les systèmes touchés pour éviter une propagation.
    - Utilisez des techniques appropriées pour préserver les preuves numériques, comme la création d'une image disque des machines affectées.
4. **Analyse Forensique :**
    - Les étudiants doivent analyser les images disques, les fichiers journaux, les captures réseau, etc., pour reconstruire la séquence des événements.
    - Identifiez les vecteurs d'attaque, les outils utilisés, et les techniques déployées par les attaquants.
    - Utilisez des outils forensiques tels que EnCase, Autopsy, ou d'autres pour extraire des informations cruciales.
5. **Rapport d'Analyse Forensique :**
    - Préparez un rapport détaillé sur l'analyse forensique, comprenant une chronologie des événements, les conclusions sur la nature de l'attaque, et les recommandations pour la résilience future.
    - Identifiez les failles de sécurité exploitées et proposez des améliorations de sécurité.
6. **Attendus et livrables :**

- Les équipes doivent présenter leurs conclusions devant un panel simulé.
- Partagez les leçons apprises, les défis rencontrés, et discutez des recommandations de sécurité.

Livrables du Projet : À la fin du projet, les étudiants devraient fournir un rapport écrit complet. Le rapport doit inclure des détails techniques, des captures d'écran, des analyses forensiques, et des recommandations concrètes. La présentation doit résumer ces informations de manière accessible pour un public non technique.

Ce projet permettra aux étudiants d'acquérir des compétences essentielles en analyse forensique tout en développant leur capacité à travailler en équipe et à présenter leurs résultats de manière claire et concise.