Lab 04

Analyse Cyber

1. Analyse d'une attaque par phishing

Contenu nécessaire :

- **Emails de phishing (exemples)** :
    - Exemple 1 corps du mail :

Un email provenant d'une "banque" demandant de mettre à jour votre mot de passe. L'URL pointe vers un domaine étrange comme "www.mysafeupdate.com".

    - Exemple 2 corps du mail :

Un email prétendant être d'un collègue, mais avec une adresse différente et demandant d'ouvrir une pièce jointe contenant un fichier malveillant.

    - Exemple 3 corps du mail :

Un email vous informant que vous avez gagné un prix, avec un lien pour réclamer le gain (vers un site douteux).

- **Instructions** :

1. Analyser les emails en mettant en évidence les éléments suspects (URL, fautes d'orthographe, urgence).
2. Identifier les actions à entreprendre pour vérifier l'authenticité de chaque email.

- **Questions pour la réflexion** :
    - Comment une entreprise peut-elle éduquer ses employés pour reconnaître ces attaques ?
    - Quels outils peuvent être utilisés pour détecter le phishing ?

2. Simulation d'attaque par ransomware

Contenu nécessaire :

- **Scénario** :
    - Le fichier confidential_data.docx est crypté par un ransomware et devient inaccessible. Un message de rançon s'affiche demandant un paiement en Bitcoin pour récupérer l'accès.
- **Instructions** :

1. Analyser les étapes pour identifier le ransomware et son fonctionnement (recherche de fichiers .exe, extensions étranges, processus en arrière-plan).

2. Utiliser un logiciel de récupération de fichiers ou des points de restauration système pour tenter de récupérer les données.

- **Outils suggérés** :
    - Outil de décryptage comme **Kaspersky Ransomware Decryptor**.
    - **RKill** (outil pour arrêter les processus malveillants).
    - **Shadow Explorer** pour explorer les versions précédentes des fichiers.
- **Questions pour la réflexion** :
    - Quelles sont les meilleures pratiques pour prévenir une attaque de ransomware ?
    - Quelle importance à la sauvegarde régulière des données ?

3. Atelier de mise en place d'une politique de sécurité

Contenu nécessaire :

- **Politique de sécurité exemple** :
    1. **Accès utilisateur** : Seuls les utilisateurs authentifiés peuvent accéder au réseau de l'entreprise via des mots de passe complexes.
    2. **Sécurisation des données** : Toutes les données sensibles doivent être chiffrées en transit et au repos.
    3. **Contrôles d'accès** : Utilisation de listes de contrôle d'accès pour restreindre l'accès aux données en fonction des rôles.
    4. **Mises à jour** : Application des patchs de sécurité dans un délai de 48 heures suivant leur disponibilité.
- **Instructions** :
    1. Rédiger une politique de sécurité en prenant en compte les besoins de l'entreprise fictive.
    2. Élaborer un plan de gestion des incidents de sécurité.
- **Questions pour la réflexion** :
    - Comment assurer la conformité des employés aux politiques de sécurité ?
    - Quelle devrait être la fréquence de révision de cette politique ?

4. Test de sécurité des mots de passe

Contenu nécessaire :

- **Liste de mots de passe à tester** :
    - Exemple 1 : 12345678
    - Exemple 2 : password123
    - Exemple 3 : qwerty!@#
    - Exemple 4 : A$12345
- **Instructions** :

1. Utiliser un outil comme **Have I Been Pwned** pour vérifier si ces mots de passe ont été compromis.

2. Créer des mots de passe robustes avec une longueur de 12 caractères minimum, comprenant des lettres majuscules, minuscules, des chiffres et des symboles.

- **Outils suggérés** : **KeePass**, **LastPass**, ou **1Password** pour la gestion sécurisée des mots de passe.
- **Questions pour la réflexion** :
    - Pourquoi utiliser un gestionnaire de mots de passe ?
    - Comment éduquer les employés à créer des mots de passe sécurisés ?

5. Analyse de logs de sécurité

Contenu nécessaire :

- **Exemple de logs (serveur web)** :

swift

CopierModifier

192.168.1.100 - - [19/Mar/2025:14:45:32 +0000] "GET /admin HTTP/1.1" 403 500 "-" "Mozilla/5.0"

192.168.1.101 - - [19/Mar/2025:14:45:33 +0000] "GET /login HTTP/1.1" 200 1200 "-" "Mozilla/5.0"

192.168.1.102 - - [19/Mar/2025:14:45:35 +0000] "POST /login HTTP/1.1" 200 1500 "login_page" "Mozilla/5.0"

- **Instructions** :
    1. Rechercher des tentatives de connexion échouées.
    2. Identifier les patterns inhabituels dans les logs.
    3. Évaluer les actions à entreprendre en cas de tentative d'intrusion.
- **Questions pour la réflexion** :
    - Pourquoi les logs sont-ils cruciaux pour la détection d'intrusions ?
    - Comment configurer des alertes pour détecter des comportements anormaux ?

6. Création d'une stratégie de sauvegarde

Contenu nécessaire :

- **Stratégie de sauvegarde exemple** :
    1. **Fréquence des sauvegardes** : Sauvegardes incrémentielles toutes les nuits, sauvegardes complètes chaque fin de semaine.
    2. **Stockage** : Sauvegardes stockées sur un NAS local et sur un cloud sécurisé.
    3. **Sécurisation** : Chiffrement des sauvegardes, stockage hors ligne.
- **Instructions** :
    1. Rédiger une stratégie de sauvegarde adaptée à une entreprise fictive.
    2. Décrire le processus de restauration des données après une attaque de ransomware.
- **Questions pour la réflexion** :
    - Quelles technologies peuvent être utilisées pour sécuriser les sauvegardes ?
    - Quel est l'impact d'une stratégie de sauvegarde mal conçue ?

7. Simuler une réponse à incident

Contenu nécessaire :

- **Scénario d'incident** :
    - Une attaque par malware a compromis un serveur critique. Les employés signalent des ralentissements dans le système et des fichiers suspects.
- **Instructions** :

1. Identifier l'attaque et la nature du malware.
2. Contenir l'incident : déconnecter les machines affectées, analyser les logs.
3. Récupérer les fichiers à partir des sauvegardes et les restaurer.
4. Documenter l'incident et préparer un rapport de réponse.

- **Questions pour la réflexion** :
    - Comment évaluer l'ampleur d'un incident de sécurité ?
    - Quels outils sont nécessaires pour effectuer une analyse post-incident ?

Livrable

- Fourniture d’un document PDF qui reprends un guide explicatif des actions effectué dans les Labs avec également des captures d’écran.