GESTION DES RISQUES INFORMATIQUES

DESS en Technologie de l'Information

EXERCICES D'APPLICATION 2

Exercice 1

1. Vrai ou Faux : Les vulnérabilités courantes

Énoncé : Indiquez si les affirmations suivantes sont vraies ou fausses. Justifiez vos réponses.

1. Un mot de passe fort doit contenir au moins 8 caractères et être composé uniquement de lettres.
2. Un pare-feu protège contre toutes les cyberattaques.
3. Ne pas mettre à jour ses logiciels expose son système à des vulnérabilités connues.
4. Le phishing est une attaque qui vise principalement les systèmes d'exploitation.

2. Trouver l'erreur de configuration

Énoncé : Parmi les scénarios suivants, identifiez la mauvaise configuration et proposez une solution.

1. Un administrateur système laisse le port 3389 ouvert sur Internet.
2. Un utilisateur conserve le mot de passe "Admin1234" sur tous ses comptes.
3. Une entreprise désactive son antivirus pour économiser des ressources système.

Exercice 2

3. Étude de cas : Attaque par ransomware

Énoncé : Une entreprise a été victime d'un ransomware exploitant une faille non corrigée de Windows.

1. Quelle erreur a été commise par l'entreprise ?
2. Quelle est la meilleure pratique pour éviter ce type d'attaque ?
3. Citez un exemple réel d'attaque de ce type.

4. Identifier une tentative de phishing

Énoncé : Voici un email reçu par un employé :

Cher client, nous avons détecté une activité suspecte sur votre compte bancaire. Cliquez sur ce lien pour vérifier vos informations immédiatement : faux-lien.com.

1. Quels indices montrent qu'il s'agit d'une tentative de phishing ?
2. Quelle est la meilleure réaction face à cet email ?

5. Mise en place d'une politique de mots de passe

Énoncé : Une entreprise souhaite renforcer la sécurité des mots de passe. Proposez une politique efficace en définissant :

1. La longueur minimale d'un mot de passe.
2. La fréquence de changement obligatoire.
3. Une méthode d'authentification complémentaire.

Exercices 3

6. Audit de sécurité d'un serveur

Énoncé : Un serveur web est accessible en ligne et contient des informations sensibles. Listez les 5 points principaux à vérifier pour garantir sa sécurité.

7. Simulation d'une attaque par force brute

Énoncé : Expliquez comment un attaquant peut utiliser un script Python pour tester des mots de passe faibles sur un serveur SSH mal configuré. Quelles mesures permettent d'atténuer cette menace ?

8. Analyse d’une attaque réelle

Énoncé : Recherchez et décrivez une cyberattaque récente impliquant une vulnérabilité courante.

1. Quel était le type de vulnérabilité exploitée ?
2. Comment les attaquants ont-ils procédé ?
3. Quelles leçons en tirer pour améliorer la cybersécurité ?