Sécurité des systèmes informatiques

TD3

Exercice 1:

Question 1

En quoi l'authentification est-elle différente de l'autorisation ?

a. L'authentification vérifie l'accès à une ressource ; l'autorisation vérifie une identité.
b. L'authentification vérifie une identité ; l'autorisation vérifie l'accès à une ressource.
c. C'est la même chose.
d. L'authentification identifie une ressource ; l'autorisation vérifie l'accès à une identité.

Question 2

Quelles sont les caractéristiques d'un mot de passe fort ? Sélectionnez toutes les réponses qui conviennent.

a. Il comprend des chiffres et des caractères spéciaux.
b. Il contient des mots du dictionnaire.
c. Il est utilisé pour tous les comptes et systèmes
d. Il contient au moins dix caractères.

Question 3

Dans un schéma d'authentification multifacteur, un mot de passe peut être considéré comme :

a. quelque chose qui vous caractérise.
b. quelque chose que vous savez.
c. quelque chose que vous avez.
d. quelque chose que vous utilisez.

Question 4

Quels sont les inconvénients de l'utilisation de la biométrie pour l'authentification ? Sélectionnez tout ce qui s'applique.

a. L'authentification biométrique est difficile ou impossible à modifier si elle est compromise.
b. Il existe des problèmes de confidentialité potentiels.
c. L'authentification biométrique est beaucoup plus lente que les autres mécanismes d'authentification.
d. La biométrie est facile à partager.

Question 5

En quoi les chalenge-responce athentifications sont-ils plus sécurisés que les générateurs OTP ?

a. Ils sont moins chers.
b. Ils résistent aux attaques de phishing.
c. Ils sont protégés par un mot de passe.
d. Ils ne peuvent pas être clonés.

Question 6

Quels sont les avantages de l'authentification unique (single sign-on offer – SSO) ? Sélectionnez tout ce qui s'applique.

a. Elle réduit le temps passé à s'authentifier.
b. Elle applique l'authentification multifacteur.
c. Elle fournit une authentification chiffrée.
d. Elle réduit le nombre total d'identifiants,

Exercice 2: Associez chaque moyen à son facteur d'authentification.
Un téléphone portable (ex : un code à usage unique envoyé par SMS).
La structure du visage.
Un mot de passe.
Une empreinte digitale.
Un code PIN de carte à puce (ex : un code de carte bancaire).
La réponse à une question secrète et connue de vous seul(e).
Une clé USB de sécurité.
La voix.
Un schéma de déverrouillage (ex : déverrouillage des smartphones).
Un générateur de mot de passe à usage unique (ex : certaines banques fournissent un boîtier pour valider des opérations bancaires comme les virements), etc.
Une empreinte rétinienne.
Une carte à puce (ex : carte bancaire, passeport électronique, carte vitale).
Un badge,
La structure de la main.

Exercice 3 :

« Je suis dans un hôtel et je dois me connecter à ma messagerie en ligne. Le seul moyen disponible pour cela est d'utiliser l'ordinateur de l'hôtel qui est en libre accès. Cette opération est-elle risquée ? »

Dans cette situation, qu'aurait-il pu arriver ?