Statut	Terminé
Commencé	jeudi 24 octobre 2024, 14:00
Terminé	jeudi 24 octobre 2024, 15:54
Durée	1 heure 54 min
Points	29,00/40,00
Note	**7,25** sur 10,00 (**72,5**%)

Question 1

Correct

Note de 1,00 sur 1,00

Propriétés de sécurité

Vous avez été recruté.e dans une grande banque et vous êtes en charge de la sécurité du service d'information qui gère les comptes clients. Votre responsable vous indique que la priorité est de réduire la fraude sur les comptes. Sur quelle propriété de sécurité devriez-vous vous concentrer.

a. Confidentialité

b. Intégrité ✓

c. Disponibilité

d. Toutes ces propriétés

Votre réponse est correcte.

La réponse correcte est :
Intégrité

Question 2

Correct

Note de 1,00 sur 1,00

Propriétés de sécurité

Vous travaillez en tant qu'expert en cybersécurité pour une entreprise qui conçoit des jeux vidéo pour cellulaire (téléphone mobile). Selon le modèle d'affaire de cette entreprise, plus les gens jouent, plus l'argent rentre. Sur quelle propriété de sécurité devriez-vous vous concentrer ?

a. Confidentialité
b. Intégrité
c. Disponibilité ✓
d. Toutes ces propriétés

Votre réponse est correcte.

La réponse correcte est :
Disponibilité

Question 3

Incorrect

Note de 0,00 sur 1,00

Propriétés de sécurité

Vous avez été recruté.e dans un hôpital comme administrateur/trice de la sécurité du système d'information qui gère les patients (dossier médical, dossier d'hospitalisation, etc.). Par ailleurs, l'hôpital compte parmi ses patients et patientes plusieurs vedettes du showbiz. Quelles sont vos priorités ?

a. Confidentialité ✗
b. Intégrité
c. Disponibilité
d. Toutes ces propriétés

Votre réponse est incorrecte.

La réponse correcte est :
Toutes ces propriétés

Question 4

Correct

Note de 1,00 sur 1,00

Analyse de risques

Tous les individus et toutes les organisations et entreprises font face aux mêmes menaces.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 5

Correct

Note de 1,00 sur 1,00

Analyse de risques

Les risques identifiés à la suite d'une analyse de risques doivent tous être traités avec la même priorité pour les éliminer.

- Vrai
- Faux ✓

La réponse correcte est « Faux ».

Question 6

Correct

Note de 1,00 sur 1,00

Analyse de risques

Dans l'entreprise Bienco, un stagiaire a l'idée d'exfiltrer des données des clients pour pouvoir les revendre sur le marché noir (darkweb). Le stagiaire souhaitant mettre toutes les chances de son côté, participe à tous les CTF pour acquérir les différentes façons d'accéder à un document sans avoir les droits dessus. Un CTF (Capture The Flag) est une compétition de cybersécurité. Chaque participant a pour mission de chercher les vulnérabilités afin de pouvoir s'introduire dans le système. L'objectif est de récupérer un drapeau, preuve que l'intrusion a réussi. Sur quel facteur d'analyse de risques ce stagiaire agit-il ?

a. Motivation

b. Intégrité

c. Opportunité

d. Capacité ✓

Votre réponse est correcte.

La réponse correcte est :
Capacité

Question 7

Correct

Note de 2,00 sur 2,00

Analyse de risques

On considère les scénarios suivants :

Scénario	Capacité	Opportunité	Motivation	Probabilité	Impact	Risque
Aline) Un employé dans un centre de données, mécontent de l'évaluation négative de sa production par sa supérieure hiérarchique, et qui n'a pas débouché pour la 5 -ème fois sur une prime, décide de se venger en s'attaquant au logiciel de climatisation des serveurs du centre pour engendrer une surchauffe des serveurs et causer une défaillance.	3	3	4	3.34	4	13,36
Brice) Un administrateur réseau et de sécurité des serveurs d'un centre de données, décide de s'attaquer au logiciel de climatisation des serveurs du centre pour engendrer une surchauffe des serveurs et causer une défaillance. Il aura auparavant exfiltré des données de ces serveurs pour les vendre au marché noir.	4	2	3	3	4	12

Laquelle des propositions suivantes est correcte.

a. La motivation de Aline est trop faible

b. Le facteur opportunité de Brice est trop faible ✓

c. L'impact des actions de Brice est trop haut

d. Le risque induit par Aline est incorrect

e. La probabilité des actions de Brice ne prend pas en compte l'impact

Votre réponse est correcte.

La réponse correcte est :
Le facteur opportunité de Brice est trop faible

Question 8

Correct

Note de 1,00 sur 1,00

Signature d'un message

Alice souhaite signer un message m faisant plusieurs méga octets.

Pour cela, elle peut utiliser une fonction de chiffrement RSA 2048 bits et une fonction de hachage SHA-256.

Quelle est la façon la plus efficace en termes de performance de signer le message m ?

a. Hacher le message m avec SHA-256

b. Hacher le message avec SHA-256, puis chiffrer le résultat avec RSA 2048 ✓

c. Chiffrer le message m avec RSA 2048, puis hacher le résultat avec SHA-26

d. Chiffrer le message m avec RSA 20248

Votre réponse est correcte.

La réponse correcte est :
Hacher le message avec SHA-256, puis chiffrer le résultat avec RSA 2048

Question 9

Correct

Note de 1,00 sur 1,00

Entropie d'une source sonore.

On considère une source sonore S1 qui génère aléatoirement une note de musique tirée parmi 4 notes possibles : DO, RE, MI, FA

On suppose que chaque note est tirée de façon parfaitement aléatoire.

On utilise la source S1 pour générer un signal sonore de longueur 10.

Quelle est l'entropie de ce signal sonore ?

a. 11 bits

b. 40 bits

c. 20 bits ✓

d. 2 bits

e. 10 bits

f. 1 bit

Votre réponse est correcte.

La réponse correcte est :
20 bits

Question 10

Incorrect

Note de 0,00 sur 1,00

Entropie d'une source sonore.

On considère une source sonore S2 qui génère aléatoirement une note de musique tirée parmi 4 notes possibles : DO, RE, MI, FA

Initialement, la première note est tirée de façon parfaitement aléatoire parmi les 4 notes.

Ensuite, la note générée par S2 est tirée de façon aléatoire de la façon suivante.

On note Val(S2,n) la note générée par la source S2 à l'étape n.

On a alors :

- Dans 50% des cas, Val(S2,n+1) = Val(S2,n) + 1
- Dans 50% des cas, Val(S2,n+1) = Val(S2,n) – 1

Avec :

- DO + 1 = RE et DO – 1 = FA
- RE + 1 = MI et RE – 1 = DO
- MI + 1 = FA et MI – 1 = RE
- FA + 1 = DO et FA – 1 = MI

Par exemple, la séquence suivante (RE – MI – RE – DO – FA – DO – RE) est une séquence de notes que peut possiblement générer la source S2

La source S2 est-elle markovienne ?

- (•) Vrai ✕
- ( ) Faux

La réponse correcte est « Faux ».

Question 11

Incorrect

Note de 0,00 sur 1,00

Entropie d'une source sonore.

La source S2 est identique à la question précédente.

On utilise la source S2 pour générer un signal sonore de longueur 10.

Quelle est l'entropie de ce signal sonore ?

a. 10 bits
b. 11 bits
c. 1 bit
d. 20 bits ✗
e. 2 bits
f. 12 bits

Votre réponse est incorrecte.

La réponse correcte est :
11 bits

Question 12

Correct

Note de 2,00 sur 2,00

Entropie d'une source sonore.

La source S2 est identique à la question précédente.

Quelle est l'entropie fréquentielle note par note de la source S2 ?

a. 1 bit
b. 11 bits
c. 2 bits ✓
d. 12 bits
e. 10 bits
f. 20 bits

Votre réponse est correcte.

La réponse correcte est :
2 bits

Question 13

Correct

Note de 2,00 sur 2,00

Entropie d'une source sonore.

La source S2 est identique à la question précédente.

Quelle est l'entropie du langage généré par la source S2 ?

- a. 1 bit ✓
- b. 2 bits
- c. 10 bits
- d. 12 bits
- e. 1,5 bit
- f. 11 bits

Votre réponse est correcte.

La réponse correcte est :
1 bit

Question 14

Correct

Note de 1,00 sur 1,00

Clé de chiffrement

On considère une clé de chiffrement K1 de 32 bits générée de façon parfaitement aléatoire.

On considère un attaquant qui peut tester 1 million de clés par seconde.

Au bout de combien de temps cet attaquant aura 15% de chance de casser cette clé ?

a. Environ 35 minutes

b. Environ 11 minutes ✓

c. Environ 1 minute

d. Environ 70 minutes

e. Environ 2 minutes

f. Environ 7 minutes

Votre réponse est correcte.

Il y a 2^32 clés à tester pour avoir 100% de chance de casser le mot de passe.

Pour avoir 15% de chance, il faut donc :

2^32 * 0,15 = 644 secondes donc moins de 11 minutes

La réponse correcte est :
Environ 11 minutes

Question 15

Correct

Note de 1,00 sur 1,00

Clé de chiffrement

Suite de la question précédente

On considère une clé de chiffrement K1 de 32 bits générée de façon parfaitement aléatoire.

Aujourd'hui, on suppose qu'un attaquant peut tester 1 million de clés par seconde.

On suppose que les capacités de calcul de l'attaquant suivent la loi de Moore, c'est-à-dire doublent tous les 18 mois.

Dans combien d'années, l'attaquant aura 15% de chance de casser cette clé de 32 bits en moins d'une seconde ?

a. Environ 20 ans

b. Environ 10 ans

c. Environ 18 ans

d. Environ 6 ans

e. Environ 7,5 ans

f. Environ 14 ans ✓

Votre réponse est correcte.

Soit n le nombres d'années. On cherche n tel que :

2^(n / 1,5) > 644

Donc n > Log2(644) * 1,5 = 13,99 années soit environ 14 années

La réponse correcte est :
Environ 14 ans

Question 16

Incorrect

Note de 0,00 sur 2,00

Clé de chiffrement

On considère une clé de chiffrement K2 de 32 bits générée de la façon suivante :

- Les 30 premiers bits sont générés de façon parfaitement aléatoire
- Pour le 31^{e} bit, il y a 80% de chance que ce soit un 1 et 20% de chance que ce soit un 0
- Pour le 32^{e} bit, il y a 80% de chance que ce soit un 0 et 20% de chance que ce soit un 1

On considère un attaquant qui peut tester 1 million de clés par seconde.

On suppose que cet attaquant suit une stratégie qui met le maximum de chances de son côté.

En suivant cette stratégie, au bout de combien temps cet attaquant aura 15% de chance de casser la clé K2 ?

a. Environ 252 secondes

b. Environ 1074 secondes

c. Environ 537 secondes

d. Environ 161 secondes ✕

Votre réponse est incorrecte.

La meilleure stratégie consiste à tester les clés se terminant par « 10 ».

En testant toutes les clés se terminant par 10, l'attaquant a 0,8 * 0,8 = 64% de chances de casser la clé.

Et il y a 2^30 clés se terminant par 10.

Le temps nécessaire pour avoir 15% de chance de casser la clé est donc :

2^30 / 1000000 * 15 / 64 = 251,7 secondes

La réponse correcte est :
Environ 252 secondes

Question 17

Incorrect

Note de 0,00 sur 2,00

Clé de chiffrement

On considère une clé de chiffrement K3 de 32 bits générée de la façon suivante :

· Pour chaque bit de la clé, il y a 90% de chance que ce soit un 0 et 10% que ce soit un 1

On considère un attaquant qui suit une stratégie qui met le maximum de chances de son côté.

En suivant cette stratégie, combien de clés cet attaquant doit-il tester pour avoir 15% de chance de casser la clé K3 ?

a. 331 clés

b. 33 clés ✕

c. 30 clés

d. 5 clés

e. 32 clés

f. 695 clés

Votre réponse est incorrecte.

On commence par tester la clé ne contenant que des 0.

La probabilité que ce soit la bonne clé : 0,9 ^32 = 3,43%

On teste ensuite les clés contenant un seul 1.

La probabilité que ce soit la bonne clé : 0,9 ^31 * 0,1 = 0,38%

Il y a 32 clés possibles ne contenant qu'un seul 1.

On cherche un nombre de clé n inférieur à 32 tel que :

3,43 + n * 0,38 > 15

Donc n > (15 – 3,43) / 0,38 = 30,45

Donc n = 31 clés

En ajoutant la clé ne contenant que des 0, la réponse est donc 32 clés

La réponse correcte est :
32 clés

Question 18

Partiellement correct

Note de 1,00 sur 2,00

Force d'une fonction de chiffrement

On considère 4 clés de chiffrement symétrique de 64 bits : K1, K2, K3 et K4

On note enc(k,m) = m' pour représenter que m' est le résultat du chiffrement du message m avec la clé k.

On considère les 4 fonctions de chiffrements suivantes :

ENC1 : enc(K2, enc(K2, enc(K1, enc(K1, m))))

ENC2 : enc(K2, enc(K1, enc(K2, enc(K1, m))))

ENC3 : enc(K1, enc(K3, enc(K2, enc(K1, m))))

ENC4 : enc(K4, enc(K3, enc(K2, enc(K1, m))))

Pour chacune des fonctions de chiffrement, on considère un attaquant qui peut réaliser une attaque à texte clair connu.

Indiquer quelle est la longueur de la clé de chiffrement symétrique équivalente à ces différentes fonctions de chiffrement :

ENC1 65 bits ✓

ENC2 128 bits ✓

ENC3 192 bits ✗

ENC4 192 bits ✗

Votre réponse est partiellement correcte.

Vous en avez sélectionné correctement 2.
La réponse correcte est :
ENC1 → 65 bits,

ENC2 → 128 bits,

ENC3 → 129 bits,

ENC4 → 129 bits

Question 19

Correct

Note de 1,00 sur 1,00

Gestion des mots de passe

Une entreprise décide de changer sa politique de gestion des mots.

Le mot de passe est généré aléatoirement dans un ensemble de caractères composés de lettres minuscules (26 caractères), lettres majuscules (26 caractères), chiffres (10 caractères) et caractères spéciaux (11 caractères).

Quel devrait être la longueur du mot de passe pour que celui-ci ait une entropie supérieure à 80 ?

- a. 10
- b. 15
- c. 13 ✓
- d. 18
- e. 8
- f. 20

Votre réponse est correcte.

Il y a 26 + 26 + 10 + 11 = 73 caractères

En appliquant Shannon, l'entropie d'un caractère est égale à Log2(73).

Pour un mot de passe de n caractères, l'entropie est donc n * Log2(73).

On cherche donc n tel que : n * Log2(73) > 80

Soit n > 80 / Log2(73) = 12,92

Donc n = 13 caractères.

La réponse correcte est :
13

Question 20

Correct

Note de 1,00 sur 1,00

Gestion des mots de passe

Suite de la question précédente.

La réponse à la question précédente est jugée trop élevée pour que les employés puissent se rappeler leur mot de passe.

L'entreprise décide donc d'opter pour des phrases de passe.

La phrase de passe sera constituée de 6 mots tirés au hasard dans un dictionnaire.

Quelle doit être la taille minimale du dictionnaire pour que la phrase de passe ait une entropie supérieure à 80 ?

a. Un peu plus de 2000 mots

b. Un peu plus de 8000 mots

c. Un peu plus de 10000 mots ✓

d. Un peu plus de 1000 mots

e. Un peu plus de 15000 mots

f. Un peu plus de 5000 mots

Votre réponse est correcte.

Soit n la taille du dictionnaire.

En appliquant Shannon, l'entropie d'un mot tirée au hasard dans ce dictionnaire est égale à Log2👎 .

Pour une phrase de passe de 6 mots, l'entropie est donc 6 * Log2👎 .

On cherche donc n tel que : 6 * Log2👎 > 80

Soit Log2👎 > 80 / 6

Donc n > 2^(80 / 6) = 10321,3 mots

Donc n = 10322 mots.

La réponse correcte est :
Un peu plus de 10000 mots

Question 21

Correct

Note de 1,00 sur 1,00

Cryptanalyse d'une clé RSA

En utilisant l'algorithme de Shor, il sera théoriquement possible avec un ordinateur quantique suffisamment puissant de casser une clé RSA par factorisation en O(n^3) ou n est la longueur de la clé.

On suppose que l'algorithme de Shor peut être exécuté en 5 * n^3 opérations et l'ordinateur quantique peut exécuter jusqu'à 10 000 000 (10^7) opérations par seconde.

Sous ces hypothèses, combien de temps serait nécessaire pour casser une clé RSA de 2048 bits ?

a. 63 heures 27 minutes et 5 secondes

b. 5 heures et 52 minutes

c. 1 heure et 11 minutes et 35 secondes ✓

d. 15 secondes

e. 12 heures 5 minutes et 10 secondes

f. 17 minutes et 12 secondes

Votre réponse est correcte.

Nombre d'opérations nécessaires pour casser la clé RSA de 2048 bits :

5 * 2048^3 = 42 949 672 960

L'ordinateur quantique peut exécuter 10^7 opérations par seconde.

Temps nécessaire pour casser la clé :

42 949 672 960 / 10^7 = 4295 secondes = 1 heure et 11 minutes et 35 secondes

La réponse correcte est :
1 heure et 11 minutes et 35 secondes

Question 22

Correct

Note de 1,00 sur 1,00

Authentification

Les jetons de mot de passe à usage unique (OTP) étaient à l'origine des dispositifs matériels, mais ils peuvent désormais être logiciels et sont devenus l'un des facteurs de l'authentification multifacteur les plus courants. Lesquelles des affirmations suivantes sont correctes ?

- [x] a. Les OTP sont constitués de caractères alphabétiques ou numériques. ✓
- [ ] b. Les OTP ne peuvent être reçus que par SMS
- [x] c. Les OTP peuvent être générés périodiquement ✓
- [x] d. Les OPT sont générés à la suite d'une requête d'authentification ✓
- [ ] e. Les propositions b et c

Votre réponse est correcte.

Les réponses correctes sont : Les OTP sont constitués de caractères alphabétiques ou numériques. ,
Les OTP peuvent être générés périodiquement,

Les OPT sont générés à la suite d'une requête d'authentification

Question 23

Correct

Note de 1,00 sur 1,00

L'authentification à un facteur est un sous ensemble de la MFA (authentification multifacteur).

- ○ Vrai
- ◉ Faux ✓

La réponse correcte est « Faux ».

Question 24

Incorrect

Note de 0,00 sur 1,00

Que faire si vous recevez deux codes de sécurité sans que vous ayez essayé de vous connecter à votre compte ? (Plusieurs réponses possibles)

- [ ] a. Vous vous connectez à votre compte et saisissez le dernier code reçu
- [ ] b. Vous vous connectez à votre compte et saisissez le premier code reçu
- [ ] c. Vous ignorer les deux codes
- [x] d. Vous contactez l'administrateur pour confirmer l'authenticité d'un des deux codes ✗
- [x] e. Vous changer votre mot de passe ✓

Votre réponse est incorrecte.

Les réponses correctes sont :
Vous ignorer les deux codes,

Vous changer votre mot de passe

Question 25

Correct

Note de 1,00 sur 1,00

Je n'ai rien de confidentiel sur mon compte, je n'ai donc pas besoin de me préoccuper de l'authentification multifacteur.

- ○ Vrai
- ◉ Faux ✓

La réponse correcte est « Faux ».

Question 26

Correct

Note de 1,00 sur 1,00

Universal 2nd Factor (U2F) est une norme ouverte qui renforce et simplifie l'authentification à deux facteurs à l'aide de périphériques spécialisés comme une USB (Universal Serial Bus) et fait appel à un protocole d'authentification à clé publique. En quoi les générateurs OTP sont-ils moins sûrs que les jetons U2F ?

a. Ils sont vulnérables à l'hameçonnage. ✓

b. Ils peuvent être clonés.

c. Ils sont beaucoup moins chers.

d. La durée de vie d'un OTP est trop courte,

Votre réponse est correcte.

La réponse correcte est :
Ils sont vulnérables à l'hameçonnage.

Question 27

Correct

Note de 1,00 sur 1,00

Pour s'authentifier avant de s'introduire dans l'enceinte d'une centrale nucléaire, Emmeline doit saisir son login mot de passe sur un clavier muni d'un écran placé à l'entrée de la centrale. Elle doit par la suite écrire, si le login-mot de passe est réussi, sur une tablette graphique, au moyen d'un stylo doté de capteurs électroniques, une phrase qui s'affiche sur l'écran accompagnant le clavier suite à son login. De quel type d'authentification s'agit-il dans ce cas ?

a. Deux facteurs ✓

b. OTP

c. Un facteur

d. Aucune de ces propositions

Votre réponse est correcte.

La réponse correcte est :
Deux facteurs

Question 28

Correct

Note de 1,00 sur 1,00

Autorisation

Parmi les propositions suivantes lesquelles sont incorrectes dans le modèle RBAC :

- a. Une permission peut être affectée à plusieurs rôles
- b. Un rôle regroupe un ensemble de permissions et d'interdictions d'accès ✓
- c. L'intersection entre les permissions de deux rôles est toujours vide ✓
- d. Un sujet peut avoir plusieurs rôles
- e. Plusieurs sujets peuvent être affectés à un rôle

Votre réponse est correcte.

Les réponses correctes sont :
Un rôle regroupe un ensemble de permissions et d'interdictions d'accès,

L'intersection entre les permissions de deux rôles est toujours vide

Question 29

Incorrect

Note de 0,00 sur 1,00

Authentification

Parmi les mots de passe suivants, lequel est le plus robuste ?

- a. Mon1erveloetaitturquoise
- b. Password12345678
- c. QXiL-2Bq3-Gu22 ✗
- d. HiP@sswd38

Votre réponse est incorrecte.

La réponse correcte est :
Mon1erveloetaitturquoise

Question 30

Correct

Note de 1,00 sur 1,00

Autorisation

Ce modèle est adapté aux environnements dynamiques car il permet des politiques de contrôle d'accès qui prennent en compte des conditions et des contextes changeants. De quel modèle de contrôle d'accès s'agit-il ?

- a. AGLP
- b. DAC
- c. Bell et Lapadula
- d. RBAC
- e. ABAC ✓

Votre réponse est correcte.

La réponse correcte est :
ABAC

Question 31

Correct

Note de 1,00 sur 1,00

Autorisation

Un fichier exécutable F1 possède le bit setuid et appartient à l'utilisateur S1. Lorsque l'utilisateur S2 exécute F1 (S2 dispose des autorisations d'exécution de F1), l'UID du processus qui exécute F1 est le suivant :

- a. S2
- b. S1 ✓

Votre réponse est correcte.

La réponse correcte est :
S1

Question 32

Correct

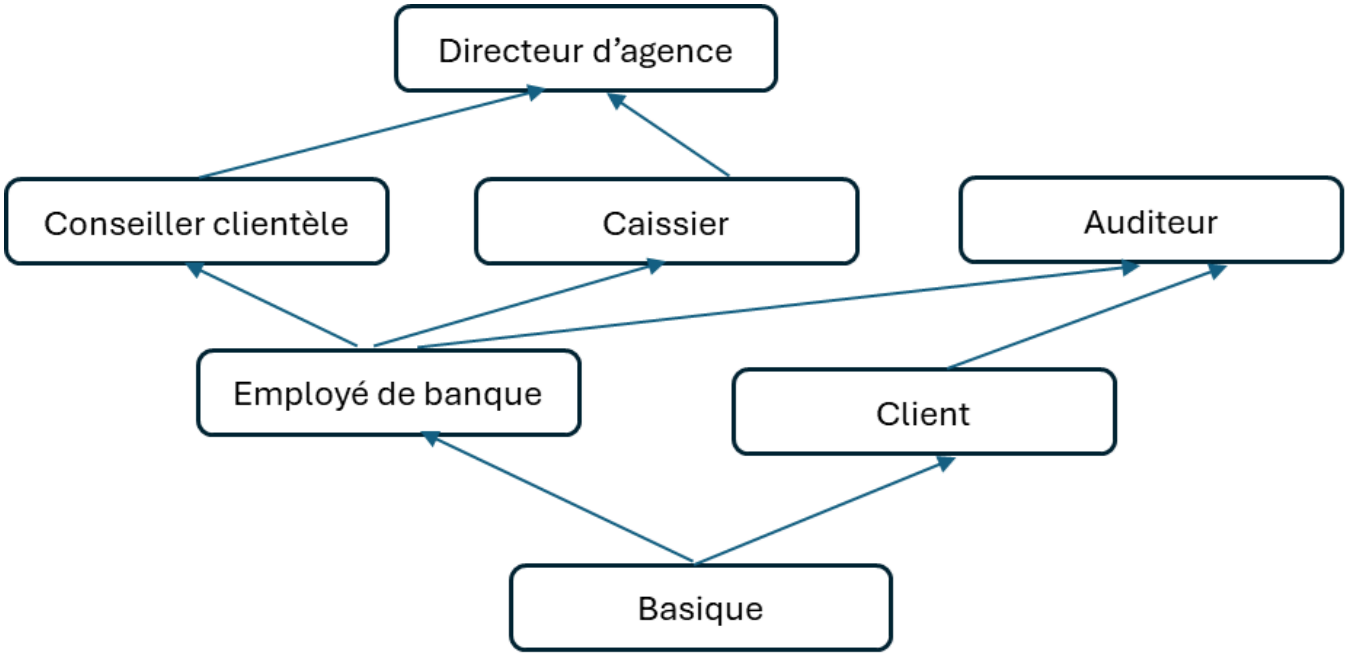
Note de 2,00 sur 2,00

Autorisation

Considérons un scénario bancaire simplifié et le modèle RBAC. On considère un ensemble de rôles, incluant le rôle client. Pour effectuer une transaction sur un compte (effectuer des dépôts et des retraits), un client utilise sa carte pour l'autoriser. Pour ce faire, il doit être enregistré dans la banque en tant que « client » à l'aide d'un lecteur de carte. Le compte de ce client est alors autorisé pour la durée de cette session, et les sujets autorisés peuvent effectuer des transactions sur ce compte. Les rôles définis dans cette banque et les droits associés, sous la forme (rôle ; droits), sont:

(Employé de banque ; Lire toutes les données du compte), (Basique ; Lire les conditions d'utilisation), (Auditeur ; Effectuer un audit), (Directeur d'agence ; Ouvrir et autoriser des transactions de compte, y compris sans carte bancaire), (Caissier ; Modifier un compte autorisé), (Conseillère clientèle ; Ouvrir un compte bancaire), (Client ; Autoriser son propre compte).

Quel lien d'héritage est erroné dans la hiérarchie de rôles proposée ci-dessous ?



a. Caissier – Directeur d'agence

b. Client – Auditeur ✓

c. Basique-Client

d. Employé de banque – Caissier

e. Conseillé clientèle – Directeur d'agence

f. Basique - Employé de banque

g. Employé de banque – Conseillé clientèle

h. Employé de banque – Auditeur

Votre réponse est correcte.

La réponse correcte est :
Client – Auditeur

Question 33

Incorrect

Note de 0,00 sur 1,00

Autorisation

Soit la matrice d'accès suivante :

	F1	F2	F3
Jean	Lire	Ajouter	Écrire
Renée	Ajouter	Écrire	-

On considère que Jean a un niveau d'habilitation ''confidentiel'' et que Renée a un niveau d'habilitation ''Secret''. On considère que le niveau de classification de F1 est ''public'', la classification de F2 est ''Secret'' et la classification de F3 est ''Top-Secret''.

Notez que public < Confidentiel < Secret < Top-Secret.

Parmi les actions suivantes, lesquelles sont autorisées ?

- a. Renée ajoute au fichier F1 ✕
- b. Renée ajoute au fichier F3
- c. Jean lit le fichier F2
- d. Jean lit le fichier F1

Votre réponse est incorrecte.

La réponse correcte est :
Jean lit le fichier F1