Commencé le	jeudi 9 mars 2023, 14:00
État	Terminé
Terminé le	jeudi 9 mars 2023, 16:00
Temps mis	1 heure 59 min
Points	25,00/40,00
Note	**6,25** sur 10,00 (**62,5**%)

Question **1**

Incorrect

Note de 0,00 sur 1,00

Un pirate réalise une attaque en brute force pour récupérer les mots de passe des employés d'une entreprise dont le PDG l'a licencié, quelle propriété de sécurité est affectée par cette attaque :

a. L'authentification ✖

b. L'intégrité

c. La disponibilité

d. La confidentialité

Votre réponse est incorrecte.

La réponse correcte est :
La confidentialité

Question **2**

Correct

Note de 1,00 sur 1,00

Le contrôle d’accès est un moyen de :

a. Cyberdéfense

b. Cyberprotection ✔

c. Cyberésilience

d. Détection d’intrusion

Votre réponse est correcte.

La réponse correcte est :
Cyberprotection

Question **3**

Incorrect

Note de 0,00 sur 2,00

Dans les données du tableau ci-dessous, on vous demande d'indiquer les deux erreurs qui s'y sont glissées,

Scénario	Capacité	Opportunité	Motivation	Probabilité	Impact	Risque
Scénario 1 : Une cybercriminelle réalise une attaque au moyen d'un cheval de Troie pour exfiltrer des données des clients d'une banque	2	2	3	2.33	4	10.68
Scénario 2 : Un collégien cybercriminel réalise une attaque au moyen d'un cheval de Troie pour exfiltrer des données des clients d'une banque	4	2	3	3	4	12

- a. L'impact dans S2 est trop élevé
- b. Le risque du scénario 1 est trop élevé
- c. Le facteur motivation dans S2 est trop élevé
- d. Le facteur capacité dans le scénario 1 est trop faible ✔
- e. Les probabilités sont incorrectes ✖

Votre réponse est incorrecte.

Les réponses correctes sont :
Le risque du scénario 1 est trop élevé,

Le facteur capacité dans le scénario 1 est trop faible

Question **4**

Correct

Note de 1,00 sur 1,00

En accédant à un site sur Internet, votre ordinateur peut être infecté par un virus, Est-ce qu'il s'agit :

a. D'une vulnérabilité ?

b. D'une contre-mesure ?

c. D'une menace ?✔

d. D'un risque ?

Votre réponse est correcte.

La réponse correcte est :
D'une menace ?

Question **5**

Correct

Note de 2,00 sur 2,00

Quels algorithmes correspondent à des algorithmes de chiffrements symétriques ? (plusieurs réponses possibles)

a. Vernam (one-time pad)✔

b. Courbe elliptique

c. DES✔

d. RSA

e. 3DES (Triple DES)✔

f. ElGamal

g. AES✔

Votre réponse est correcte.

Les réponses correctes sont :
DES,

3DES (Triple DES),

AES,

Vernam (one-time pad)

Question **6**

Correct

Note de 1,00 sur 1,00

Lorsqu'un ordinateur quantique permettant des calculs sur plusieurs milliers de Qbits (bits quantiques) sera disponible, laquelle de ces affirmations sera vraie :

a. Il faudra remplacer les algorithmes de chiffrement symétrique par les algorithmes de chiffrement asymétrique

b. Il faudra multiplier par 2 la longueur des clés des algorithmes de chiffrement symétrique comme AES ✔

c. Aucune de ces réponses, l'ordinateur quantique n'a pas d'effet sur les algorithmes de chiffrement symétrique

d. Il faudra remplacer les algorithmes de chiffrement symétrique par les algorithmes de chiffrement post-quantique

Votre réponse est correcte.

La réponse correcte est :
Il faudra multiplier par 2 la longueur des clés des algorithmes de chiffrement symétrique comme AES

Question **7**

Correct

Note de 1,00 sur 1,00

Lorsqu'un ordinateur quantique permettant des calculs sur plusieurs milliers de Qbits (bits quantiques) sera disponible, laquelle de ces affirmations sera vraie :

a. Aucune de ces réponses, l'ordinateur quantique n'a pas d'effet sur les algorithmes de chiffrement asymétrique

b. Il faudra multiplier par 3 la longueur des clés des algorithmes de chiffrement asymétrique comme RSA

c. Il faudra remplacer les algorithmes de chiffrement asymétrique par les algorithmes de chiffrement post-quantique ✔

d. Il faudra remplacer les algorithmes de chiffrement asymétrique par les algorithmes de chiffrement symétrique

Votre réponse est correcte.

La réponse correcte est :
Il faudra remplacer les algorithmes de chiffrement asymétrique par les algorithmes de chiffrement post-quantique

Question **8**

Correct

Note de 1,00 sur 1,00

Alice envoie un message signé à Bob en utilisant l'algorithme RSA. Quelle opération doit utiliser Bob pour vérifier la signature d'Alice ?

a. Déchiffrer le message avec la clé privée d'Alice

b. Déchiffrer le message avec la clé publique d'Alice ✔

c. Déchiffrer le message avec sa clé privée

d. Déchiffrer le message avec sa clé publique

Votre réponse est correcte.

La réponse correcte est :
Déchiffrer le message avec la clé publique d'Alice

Question **9**

Correct

Note de 2,00 sur 2,00

Dans l'algorithme RSA, quel est l'algorithme généralement utilisé pour vérifier qu'un très grand nombre est premier :

a. Le crible d'Ératosthène

b. L'algorithme d'Euclide

c. L'algorithme de Polar

d. Le test de primalité probabiliste ✔

Votre réponse est correcte.

La réponse correcte est :
Le test de primalité probabiliste

Question **10**

Correct

Note de 1,00 sur 1,00

Quelle est l'entropie d'un mot de passe composé de 8 caractères (lettres minuscules a-z, majuscules A-Z et chiffres 0-9) choisis au hasard ?

a. Environ 59,5

b. Environ 35,7

c. Environ 32,5

d. Environ 47,6✔

Votre réponse est correcte.

Réponse :

Il y a 62 possibilités pour chaque caractère

L'entropie de chaque caractère est égale à (formule de Shannon) :

Log2(62) = 5,954

Entropie d'un mot de passe (8 caractères, source markovienne) :

8 * 5,954 = 47,63

La réponse correcte est :
Environ 47,6

Question **11**

Correct

Note de 1,00 sur 1,00

Deux politiques de gestion des mots de passe sont considérées :

1) choisir un mot de passe composé de 8 caractères (lettres minuscules a-z, majuscules A-Z et chiffres 0-9) choisis au hasard et

2) choisir une « phrase » de passe composée de quatre mots du français courant, choisis au hasard dans un dictionnaire de 6 000 mots.

On considère un attaquant qui a accès au dictionnaire utilisé pour générer la phrase de passe dans la politique 2).

Face à une attaque par force brute, quelle affirmation est vraie ?

- a. L'attaquant doit tester environ 6 fois plus de combinaisons pour casser la phrase de passe ✔
- b. L'attaquant doit tester environ 6000 fois plus de combinaisons pour casser la phrase de passe
- c. L'attaquant doit tester environ 600 fois plus de combinaisons pour casser la phrase de passe
- d. L'attaquant doit tester environ 60 fois plus de combinaisons pour casser la phrase de passe

Votre réponse est correcte.

Réponse :

Nombre de mots de passe à tester :

62 ^ 8 = 218 340 105 584 896

Nombre de phrases de passe à tester :

6000 ^4 = 1 296 000 000 000 000

1 296 000 000 000 000 / 218 340 105 584 896 = 5,935

Soit environ 6 fois plus de combinaisons pour casser la phrase de passe

La réponse correcte est :
L'attaquant doit tester environ 6 fois plus de combinaisons pour casser la phrase de passe

Question **12**

Correct

Note de 1,00 sur 1,00

On considère une phrase de passe composée de quatre mots du français courant, choisis au hasard dans un dictionnaire de 6 000 mots.

Un attaquant a accès au dictionnaire utilisé pour générer la phrase de passe et réalise une attaque par force brute.

Cet attaquant peut tester 10 000 000 000 (dix milliards) de phrases de passe à la seconde.

Quelles sont les chances de l'attaquant de casser le mot de passe au bout d'une journée ?

a. Une chance sur trois

b. 100% de chance

c. Une chance sur deux

d. Deux chances sur trois ✔

Votre réponse est correcte.

Réponse :

Nombre de phrase de passe à tester pour avoir 100% de chance :

6000 ^4 = 1 296 000 000 000 000

Nombre de mots de passe testés au bout d'une journée :

10 000 000 000 * 60 * 60 * 24 = 864 000 000 000 000

Probabilité de casser le mot de passe au bout d'un jour :

864 000 000 000 000 / 1 296 000 000 000 000 = 0,66

Soit 2 chances sur 3

La réponse correcte est :
Deux chances sur trois

Question **13**

Correct

Note de 1,00 sur 1,00

On considère un dictionnaire qui contient 6000 mots : 3000 mots de 6 lettres et 3000 mots de 7 lettres.

On considère un générateur G de mots de passe qui fonctionne de la façon suivante :

Un mot est choisi au hasard dans le dictionnaire.

Si le mot choisi fait 7 lettres, alors le mot est complété par un chiffre de 0 à 9.

Si le mot choisi fait 6 lettres, alors le mot est complété par deux chiffres de 0 à 9.

Par exemple si « moteur » (6 lettres) et « machine » (7 lettres) sont deux mots appartenant au dictionnaire, alors moteur8 et machine92 sont des mots de passe que peut possiblement générer G.

Combien de mots de passe différents peut générer G ?

- a. 30 000
- b. 600 000
- c. 6 000
- d. 60 000
- e. 33 000
- f. 330 000 ✔

Votre réponse est correcte.

Réponse :

Si le mot choisi dans le dictionnaire est de 7 lettres (3000 mots possibles), alors G peut générer 3000 * 10 mots de passe différents, soit 30 000 mots de passe.

Si le mot choisi dans le dictionnaire est de 6 lettres (3000 mots possibles), alors G peut générer 3000 * 100 mots de passe différents, soit 300 000 mots de passe.

Au total, G peut donc générer 30 000 + 300 000 = 330 000 mots de passe différents.

La réponse correcte est :
330 000

Question **14**

Correct

Note de 1,00 sur 1,00

On considère le même générateur G de mots de passe que dans la question précédente :

Un mot est choisi au hasard dans un dictionnaire qui contient 6000 mots : 3000 mots de 6 lettres et 3000 mots de 7 lettres.

Si le mot choisi fait 7 lettres, alors le mot est complété par un chiffre de 0 à 9.

Si le mot choisi fait 6 lettres, alors le mot est complété par deux chiffres de 0 à 9.

Tous les mots de passe générés par G ont la même probabilité d'être générés.

Veuillez choisir une réponse.

- Vrai
- Faux ✔

Réponse : Faux

Dans la première étape, il y a autant de chance de choisir un mot de 6 lettres dans le dictionnaire qu'un mot de 7 lettres.

Dans la seconde étape, on peut forger 10 mots de passe si un mot de 7 lettres est choisi et 100 mots de passe si un mot de 6 lettres est choisi.

Au final, la probabilité d'avoir un mot de passe de 7 lettres avec un chiffre particulier est donc 10 fois plus grande que celle d'avoir un mot de passe de 6 lettres avec deux chiffres particuliers.

La réponse correcte est « Faux ».

Question **15**

Incorrect

Note de 0,00 sur 1,00

On considère le même générateur G de mots de passe que dans la question précédente :

Un mot est choisi au hasard dans un dictionnaire qui contient 6000 mots : 3000 mots de 6 lettres et 3000 mots de 7 lettres.

Si le mot choisi fait 7 lettres, alors le mot est complété par un chiffre de 0 à 9.

Si le mot choisi fait 6 lettres, alors le mot est complété par deux chiffres de 0 à 9.

Soit m1 un mot de 7 lettres appartenant au dictionnaire utilisé par G.

Soit M1 un mot de passe généré à partir de m1 en ajoutant un chiffre de 0 à 9.

Quelle est la probabilité que M1 soit généré par G ?

a. Une chance sur 33 000

b. Une chance sur 600 000

c. Une chance sur 30 000 ✖

d. Une chance sur 330 000

e. Une chance sur 60 000

f. Une chance sur 6 000

Votre réponse est incorrecte.

Réponse :

Il y a 50% de chance qu'un mot de 7 lettres soit choisi dans le dictionnaire.

G peut forger 30000 mots de passe à partir des 3000 mots de 7 lettres.

La probabilité que M1 soit générée par G est donc : ½ * 1 / 30000 = 1 / 60000

La bonne réponse est donc une chance sur 60 000

La réponse correcte est :
Une chance sur 60 000

Question **16**

Incorrect

Note de 0,00 sur 1,00

On considère le même générateur G de mots de passe que dans la question précédente :

Un mot est choisi au hasard dans un dictionnaire qui contient 6000 mots : 3000 mots de 6 lettres et 3000 mots de 7 lettres.

Si le mot choisi fait 7 lettres, alors le mot est complété par un chiffre de 0 à 9.

Si le mot choisi fait 6 lettres, alors le mot est complété par deux chiffres de 0 à 9.

Soit m2 un mot de 6 lettres appartenant au dictionnaire utilisé par G.

Soit M2 un mot de passe généré à partir de m2 en ajoutant deux chiffres de 0 à 9.

Quelle est la probabilité que M2 soit généré par G ?

- a. Une chance sur 330 000 ✖
- b. Une chance sur 30 000
- c. Une chance sur 6 000
- d. Une chance sur 33 000
- e. Une chance sur 60 000
- f. Une chance sur 600 000

Votre réponse est incorrecte.

Réponse :

Il y a 50% de chance qu'un mot de 6 lettres soit choisi dans le dictionnaire.

G peut forger 300 000 mots de passe à partir des mots de 6 lettres.

La probabilité que M2 soit généré par G est donc : ½ * 1 / 300000 = 1 / 600000

La bonne réponse est donc une chance sur 600 000

La réponse correcte est :
Une chance sur 600 000

Question **17**

Incorrect

Note de 0,00 sur 1,00

On considère le même générateur G de mots de passe que dans la question précédente :

Un mot est choisi au hasard dans un dictionnaire qui contient 6000 mots : 3000 mots de 6 lettres et 3000 mots de 7 lettres.

Si le mot choisi fait 7 lettres, alors le mot est complété par un chiffre de 0 à 9.

Si le mot choisi fait 6 lettres, alors le mot est complété par deux chiffres de 0 à 9.

Quelle est l'entropie moyenne d'un mot de passe généré par G ?

- a. 18,33
- b. 17,53
- c. 15,87 ✖
- d. 19,19

Votre réponse est incorrecte.

Réponse :

On applique la formule de Shannon (P1 et P2 correspondent respectivement aux probabilités calculées dans les deux questions précédentes) :

H(G) = somme{1 à 30000} P1 * Log(1/P1) + somme{1 à 300000} P2 * Log(1/P2)

Donc H(G) = ½ Log2(60000) + ½ Log2(600000) = 15,87 / 2 + 19,19 / 2 = 17, 53

La réponse correcte est :
17,53

Question **18**

Incorrect

Note de 0,00 sur 1,00

On considère le même générateur G de mots de passe que dans la question précédente :

Un mot est choisi au hasard dans un dictionnaire qui contient 6000 mots : 3000 mots de 6 lettres et 3000 mots de 7 lettres.

Si le mot choisi fait 7 lettres, alors le mot est complété par un chiffre de 0 à 9.

Si le mot choisi fait 6 lettres, alors le mot est complété par deux chiffres de 0 à 9.

Un attaquant effectue une attaque par force brute pour casser un mot de passe généré par G.

On suppose que cet attaquant sait comment G fonctionne et a accès au dictionnaire utilisé par G pour générer les mots de passe.

Si l'on suppose que l'attaquant ne dispose pas du temps suffisant pour tester tous les mots de passe possibles, quelles sont les meilleures chances que cet attaquant casse le mot de passe ?

a. En commençant par tester les mots de passe contenant un 0 (zéro)

b. Peu importe, on peut tester les mots de passe au hasard

c. En commençant par tester les mots de passe générés à partir des mots de 6 lettres du dictionnaire ✖

d. En commençant par tester les mots de passe générés à partir des mots de 7 lettres du dictionnaire

Votre réponse est incorrecte.

Réponse :

Comme la probabilité est plus grande qu'un mot de passe soit généré à partir de mots de 7 lettres, il vaut mieux commencer par tester ces mots de passe en premier.

La réponse correcte est :
En commençant par tester les mots de passe générés à partir des mots de 7 lettres du dictionnaire

Question **19**

Incorrect

Note de 0,00 sur 2,00

On considère le même générateur G de mots de passe que dans la question précédente :

Un mot est choisi au hasard dans un dictionnaire qui contient 6000 mots : 3000 mots de 6 lettres et 3000 mots de 7 lettres.

Si le mot choisi fait 7 lettres, alors le mot est complété par un chiffre de 0 à 9.

Si le mot choisi fait 6 lettres, alors le mot est complété par deux chiffres de 0 à 9.

Un attaquant effectue une attaque par force brute pour casser un mot de passe généré par G.

On suppose que cet attaquant sait comment G fonctionne et a accès au dictionnaire utilisé par G pour générer les mots de passe.

L'attaquant peut tester 1000 mots de passe par seconde.

Quelles sont les meilleures chances que cet attaquant casse le mot de passe au bout de 15 secondes ?

a. Une chance sur 4

b. Une chance sur 2

c. Une chance sur 3

d. Moins d'une chance sur 10 ✖

e. 100% de chance

Votre réponse est incorrecte.

Réponse :

G peut générer 30 000 mots de passe différents à partir des mots de passe de 7 lettres du dictionnaire.

Si l'attaquant parvient à tester ces 30 000 mots de passe, il a 50% de chance de casser le mot de passe.

Mais, en 15 secondes, l'attaquant peut seulement tester 1000 * 15 = 15 000 mots de passe.

Il a donc 25% de chance de casser le mot de passe, soit une chance sur 4.

La réponse correcte est :
Une chance sur 4

Question **20**

Incorrect

Note de 0,00 sur 2,00

On considère le même générateur G de mots de passe que dans la question précédente :

Un mot est choisi au hasard dans un dictionnaire qui contient 6000 mots : 3000 mots de 6 lettres et 3000 mots de 7 lettres.

Si le mot choisi fait 7 lettres, alors le mot est complété par un chiffre de 0 à 9.

Si le mot choisi fait 6 lettres, alors le mot est complété par deux chiffres de 0 à 9.

Un attaquant effectue une attaque par force brute pour casser un mot de passe généré par G.

On suppose que cet attaquant sait comment G fonctionne et a accès au dictionnaire utilisé par G pour générer les mots de passe.

L'attaquant peut tester 1000 mots de passe par seconde.

De combien de temps l'attaquant a-t-il besoin au minimum pour avoir 75% de chance de casser le mot de passe ?

- a. 4 minutes et 7,5 secondes ✖
- b. 5 minutes et 30 secondes
- c. 2 minutes
- d. 1 minute
- e. 11 minutes
- f. 3 minutes

Votre réponse est incorrecte.

Réponse :

G peut générer 30 000 mots de passe différents à partir des mots de passe de 7 lettres du dictionnaire.

L'attaquant a besoin de 30 secondes pour tester ces 30 000 mots de passe. Il a alors 50% de chance de casser le mot de passe.

G peut générer 300 000 mots de passe différents à partir des mots de passe de 6 lettres du dictionnaire.

Si l'attaquant parvient à tester ces 300 000 mots de passe, il a aussi 50% de chance de casser le mot de passe.

En testant la moitié de ces mots de passe, il a donc 25% de chance de casser le mot de passe.

Pour avoir 75% de chance de casser le mot de passe, l'attaquant a besoin de 30 secondes pour tester les 30 000 mots (mots de passe générés à partir des mots de 7 lettres) et de 150 secondes supplémentaires pour tester 150 000 mots de passe (moitié des mots de passe générés à partir des mots de 6 lettres).

Au total 30 + 150 = 180 secondes = 3 minutes

La réponse correcte est :
3 minutes

Question **21**

Correct

Note de 1,00 sur 1,00

Pour authentifier Bob, Alice procède de la façon suivante :

Alice partage avec Bob un code secret de 4 chiffres.

Alice génère un nombre aléatoire de 4 chiffres et l'envoie à Bob.

Bob effectue une addition modulo 10 chiffre à chiffre entre le nombre aléatoire qu'il a reçu et le code secret.

Bob renvoie le résultat de cette addition modulo 10 à Alice.

Alice effectue le même calcul que Bob. Si le résultat obtenu est identique au nombre renvoyé par Bob, alors Bob est authentifié.

Qu'elle est le mode d'authentification utilisé par Alice :

- a. One Time Password local
- b. One Time Password distant
- c. Preuve à connaissance nulle
- d. Système défi-réponse ✔

Votre réponse est correcte.

La réponse correcte est :
Système défi-réponse

Question **22**

Incorrect

Note de 0,00 sur 1,00

Dans la question précédente, quel type d'algorithme cryptographique est utilisé par Alice et Bob.

- a. Algorithme de Vigénère
- b. Algorithme de Diffie-Hellman ✖
- c. DES
- d. Algorithme de César

Votre réponse est incorrecte.

La réponse correcte est :
Algorithme de Vigénère

Question **23**

Correct

Note de 1,00 sur 1,00

Dans la question précédente, l'algorithme cryptographique utilisé par Alice et Bob fournit un bon niveau de diffusion.

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **24**

Correct

Note de 2,00 sur 2,00

Dans la question précédente, Eve parvient à intercepter le message A = 8240 envoyé par Alice ainsi que la réponse B = 7541 renvoyé par Bob.

Quelle est la clé partagée par Alice et Bob ?

- a. 5781
- b. 1389
- c. 1709
- d. 9301 ✔

Votre réponse est correcte.

Réponse :

Si K est la clé partagée par Alice et Bob alors A + K = B où « + » représente l'addition chiffre à chiffre modulo 10.

Il faut faire la soustraction chiffre modulo 10 pour obtenir K : K = B - A

On obtient K = 9301

La réponse correcte est :
9301

Question **25**

Incorrect

Note de 0,00 sur 2,00

Question 14 :

Dans la question précédente, quel est le type d'attaque réalisé par Eve :

- a. Attaque à texte clair connu
- b. Attaque par dictionnaire
- c. Attaque à texte clair choisi
- d. Attaque à texte chiffré choisi ✖
- e. Attaque sur texte chiffré seul

Votre réponse est incorrecte.

La réponse correcte est :
Attaque à texte clair connu

Question **26**

Correct

Note de 1,00 sur 1,00

Une entreprise utilise une authentification par badge pour authentifier ses employés lorsqu'ils accèdent aux locaux de l'entreprise.

Cette entreprise constate plusieurs cas d'intrusion dans ses locaux par des personnes qui ne sont pas employées par l'entreprise.

L'entreprise décide donc de combiner l'authentification par badge avec un deuxième mode d'authentification biométrique, par exemple par reconnaissance d'empreintes digitales.

Quels sont les deux modes d'authentification utilisés par cette entreprise :

- a. Quelque chose que je suis et quelque chose que je fais
- b. Quelque chose que je possède et quelque chose que je fais
- c. Quelque chose que je fais et quelque chose que je sais
- d. Quelque chose que je possède et quelque chose que je suis ✔
- e. Quelque chose que je sais et quelque chose que je possède

Votre réponse est correcte.

La réponse correcte est :
Quelque chose que je possède et quelque chose que je suis

Question **27**

Correct

Note de 1,00 sur 1,00

Dans la question précédente, l'entreprise sélectionne deux solutions biométriques :

· Solution A par reconnaissance d'empreinte digitale. La probabilité de compromission de cette solution est de 10^{-9} et le prix de cette solution est de 1000$.

· Solution B par reconnaissance d'iris. La probabilité de compromission de cette solution est de 10^{-12} et le prix de cette solution est de 5000$.

Quelle est la solution qui permet la meilleure réduction du risque de compromission de la fonction d'authentification ?

a. La solution A

b. Il manque des informations pour répondre à cette question

c. La solution B ✔

Votre réponse est correcte.

La réponse correcte est :
La solution B

Question **28**

Correct

Note de 1,00 sur 1,00

Suite de la question précédente

L'entreprise sélectionne deux solutions biométriques :

· Solution A par reconnaissance d'empreinte digitale. La probabilité de compromission de cette solution est de 10^{-9} et le prix de cette solution est de 1000$.

· Solution B par reconnaissance d'iris. La probabilité de compromission de cette solution est de 10^{-12} et le prix de cette solution est de 5000$.

On vous demande de choisir entre la solution A et la solution B. Quelle est votre choix ?

a. La solution B

b. La solution A

c. Il manque des informations pour répondre à cette question ✔

Votre réponse est correcte.

Réponse : Pour répondre à cette question, il faut évaluer l'impact pour l'entreprise de la compromission de la fonction d'authentification. Sans cette information, on peut seulement dire que la solution B permet une meilleure réduction de ce risque que la solution A. Mais, le coût d'achat la solution B est plus élevé que celui de la solution A. On ne peut donc pas décider quelle solution choisir sans connaître l'impact de la compromission.

La réponse correcte est :
Il manque des informations pour répondre à cette question

Question **29**

Correct

Note de 1,00 sur 1,00

Suite de la question précédente

L'entreprise choisit de s'équiper d'un système de reconnaissance d'empreinte digitale.

Un attaquant pourrait parvenir à voler le badge d'un employé et à fabriquer des prothèses pour imiter les empreintes digitales de cet employé

Est-ce qu'il s'agit ?

a. D'une menace

b. D'un risque résiduel ✔

c. D'une contre-mesure

d. D'une vulnérabilité

Votre réponse est correcte.

La réponse correcte est :
D'un risque résiduel

Question **30**

Correct

Note de 1,00 sur 1,00

Dans le modèle RBAC, Les contraintes de type DSOD (Dynamic Separation Of Duties) ne peuvent être spécifiées dans une politique d'accès d'un système cible contenant déjà des contraintes de type SSOD (Static Separation Of Duties), elles ne peuvent pas coexister.

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

Question **31**

Partiellement correct

Note de 1,00 sur 2,00

Soit la matrice discrétionnaire suivante,

	F1	F2	F3	F4
S1	RW	RW	R	-
S2	-	R	RW	-
S3	R	-	R	R

On suppose que les sujets S1, S2 et S3 peuvent utiliser des applications malveillantes pour transférer illégalement le contenu des fichiers.

Lesquelles de ces trois propositions suivantes sont correctes ? (plusieurs réponses possibles)

- [ ] a. S2 peut lire F1
- [x] b. S3 peut lire F2 ✔
- [ ] c. S2 peut lire F4
- [ ] d. S1 peut lire F4

Votre réponse est partiellement correcte.

Vous en avez sélectionné correctement 1.
Les réponses correctes sont :
S3 peut lire F2,

S2 peut lire F1

Question **32**

Correct

Note de 1,00 sur 1,00

Emilie et Samia sont toutes deux d'habilitation « confidentiel». Chacune d'entre-elles a son compte informatique hébergé par un système géré par un mécanisme de type Bell et Lapadula. Emilie chiffre un message et l'envoie à Samia. Laquelle de ces propositions est correcte :

- ( ) a. Samia reçoit le message chiffré mais ne peut le déchiffrer
- (•) b. Emilie ne peut pas envoyer le message à Samia en utilisant Internet ✔
- ( ) c. Samia renvoie un accusé de réception chiffré à Emilie

Votre réponse est correcte.

La réponse correcte est :
Emilie ne peut pas envoyer le message à Samia en utilisant Internet