Commencé le	jeudi 11 mars 2021, 14:27
État	Terminé
Terminé le	jeudi 11 mars 2021, 15:33
Temps mis	1 heure 6 min
Points	26,00/27,00
Note	**28,89** sur 30,00 (**96**%)

Question **1**

Correct

Note de 1,00 sur 1,00

Pour que le chiffrement de Vernam soit parfaitement sécuritaire, il faut utiliser une clé aléatoire de la même longueur que le message que l'on veut chiffrer.

Sélectionnez une réponse :

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question **2**

Correct

Note de 1,00 sur 1,00

Dans les distributions Linux modernes, les informations sur les mots de passe des usagers se trouvent dans le fichier /etc/passwd.

Sélectionnez une réponse :

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **3**

Correct

Note de 1,00 sur 1,00

Lors de l'analyse de risque en sécurité informatique, il est nécessaire d'établir le scénario à travers lequel un attaquant pourrait conduire des actions qui atteindrait aux objectifs de sécurité (le « comment »), mais il n'est pas nécessaire de préciser qui cet attaquant serait.

Sélectionnez une réponse :

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **4**

Correct

Note de 1,00 sur 1,00

L'utilisation d'une méthode d'authentification par « défi-réponse » ("challenge-response", en anglais) permet de se protéger contre l'interception de la session d'authentification

Sélectionnez une réponse :

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question **5**

Correct

Note de 1,00 sur 1,00

Complétez la phrase, un risque est la combinaison _____ et d'une menace ?

- a. d'une vulnérabilité ✔
- b. d'une attaque
- c. d'un scénario
- d. d'un attaquant

Votre réponse est correcte.

La réponse correcte est :
d'une vulnérabilité

Question **6**

Correct

Note de 1,00 sur 1,00

Lorsqu'un acteur malveillant récupère ou vole le SecureID d'authentification d'un employé d'une compagnie qu'il souhaite attaquer, lequel des attributs suivants de l'analyse de risque est affecté :

- a. Opportunité ✔
- b. Motivation
- c. Intégrité
- d. Capacité

Votre réponse est correcte.

La réponse correcte est :
Opportunité

Question **7**

Correct

Note de 1,00 sur 1,00

Dans un cyber café

Un utilisateur malveillant s'installe dans un cyber café et essaye d'intercepter des mots de passe et numéros de carte de crédit sur le réseau Wi-Fi du café pour réaliser de la fraude bancaire par Internet.

Est-ce qu'il s'agit :

- a. D'une menace ? ✔
- b. D'un risque ?
- c. D'une vulnérabilité ?
- d. D'une contre-mesure ?

Votre réponse est correcte.

La réponse correcte est :
D'une menace ?

Question **8**

Correct

Note de 1,00 sur 1,00

Quelle est l'erreur dans l'analyse de risque suivante ?

Scénario	Capacité	Opportunité	Motivation	Probabilité	Impact	Risque
A) Un cyber criminel réalise une attaque Man in the Middle sur le protocole HTTP pour réaliser une fraude bancaire	3	2	3	2.67	4	10.67
B) Un usager typique réalise une attaque Man in the Middle sur le protocole HTTP pour réaliser une fraude bancaire	4	2	3	3	4	12

- a. Le calcul du risque ne prend pas en compte la probabilité
- b. L'impact dans B est trop élevé
- c. La capacité dans B est trop élevé ✔
- d. L'opportunité de B est trop élevé
- e. La motivation dans B est trop élevé

Votre réponse est correcte.

La réponse correcte est :
La capacité dans B est trop élevé

Question **9**

Correct

Note de 1,00 sur 1,00

Après avoir fait votre analyse de risque telle que vu en classe, vous constatez que la menace A démontre un risque de 2.1 dans votre échelle quantitative, tandis que vous évaluez la menace B à un risque calculé de 4.2. Que pouvez-vous conclure sur le risque des menaces A et B? Choisissez la meilleure réponse.

- a. La menace B est plus risquée que la menace A ✔
- b. Les risques reliés aux menaces A et B sont acceptables
- c. La menace B est deux fois plus risquée que la menace A
- d. La menace A est plus risquée que la menace B
- e. La menace A est deux fois plus risquée que la menace B

Votre réponse est correcte.

La réponse correcte est :
La menace B est plus risquée que la menace A

Question **10**

Incorrect

Note de 0,00 sur 1,00

La loi de Moore stipule que la puissance de calcul des ordinateurs disponibles sur le marché double à chaque 18 mois. Combien de bits de clés serait-il nécessaire d'ajouter à un algorithme de cryptographie symétrique à 128 bits pour compenser pour l'effet de la Loi de Moore sur une période de 15 ans.

- a. 10 bits
- b. 15 bits ✖
- c. 128 bits
- d. Il n'est pas nécessaire d'augmenter la taille de la clé

Votre réponse est incorrecte.

La réponse correcte est :
10 bits

Question **11**

Correct

Note de 1,00 sur 1,00

On considère une source qui génère aléatoirement trois chiffres possibles 0, 1 et 2. La probabilité d'apparition du 0 est ½ et celle d'apparition du 1 est ¼ et celle du 2 est également ¼. On utilise cette source pour générer une chaine de 10 chiffres. Quelle est l'entropie de cette chaîne :

- a. 15,8 bits
- b. 1 bit
- c. 1,5 bit
- d. 1,58 bit
- e. 10 bits
- f. 15 bits ✔

Votre réponse est correcte.

On applique la formule pour calculer l'entropie de la source :

$H(S) = 1/2 * \log2(2) + 1/4 * \log2(4) + 1/4 * \log2(4)$

$= 1/2 + 1/2 + 1/2 = 1,5$ bits

Comme la source est markovienne (source aléatoire sans mémoire), il suffit de multiplier par 10 pour avoir l'entropie du message :

$10 * 1,5 = 15$bits

La réponse correcte est :
15 bits

Question **12**

Correct

Note de 1,00 sur 1,00

Dans l'étape 3 du processus de gestion du risque de sécurité informatique, vous avez identifié pour une menace X trois possibles contre mesures A, B et C qui réduisent le risque relié à cette menace. Laquelle de ces informations est la moins pertinente dans le choix de la meilleure contre mesure à déployer :

- a. La contre mesure C s'est avérée efficace lors de son introduction dans le marché de la sécurité informatique il y a une vingtaine d'années, et est aujourd'hui est toujours très largement utilisée ✔
- b. Le coût d'achat de la contre mesure A est supérieur à celui de B et de C
- c. Votre assureur en risque informatique offre une réduction de prime d'assurance si vous choisissez d'installer C
- d. Le responsable de sécurité informatique d'une autre compagnie similaire vous indique que les usagers de son entreprise se sont plaint du manque de convivialité et de la perte de temps engendrée par le déploiement de la contre mesure B

Votre réponse est correcte.

La réponse correcte est :
La contre mesure C s'est avérée efficace lors de son introduction dans le marché de la sécurité informatique il y a une vingtaine d'années, et est aujourd'hui est toujours très largement utilisée

Question **13**

Correct

Note de 1,00 sur 1,00

Nous sommes en 2050 et il n'est plus recommandé d'utiliser le protocole AES avec une clé de 128 bits. Votre directeur vous demande de comparer deux solutions : (1) chiffrer les documents une deuxième fois avec une autre clé de 128 bits, (2) déchiffrer tous les documents et les rechiffrer avec une clé de 256 bits. Vous répondez :

- a. La solution 2 est préférable ✔
- b. La solution 1 est préférable
- c. Les deux solutions sont équivalentes

Votre réponse est correcte.

La réponse correcte est :
La solution 2 est préférable

Question **14**

Correct

Note de 1,00 sur 1,00

Avec le protocole RSA, pour vérifier un message signé par Alice, Bob doit utiliser :

- a. La clé privée d'Alice
- b. Sa propre clé publique
- c. Sa propre clé privée
- d. La clé publique d'Alice ✔

Votre réponse est correcte.

La réponse correcte est :
La clé publique d'Alice

Question **15**

Correct

Note de 1,00 sur 1,00

Laquelle de ces conditions **n'est pas** nécessaire pour assurer la sécurité d'un système de signature numérique avec hachage cryptographique :

- a. Une entropie élevée de la source qui génère les textes à signer ✔
- b. Une fonction de hachage pour laquelle il est difficile de trouver des collisions avec un haché donné
- c. Un algorithme à clé publique pour lequel il est très difficile de trouver la clé privée à partir de la clé publique
- d. Un mécanisme permettant d'assurer au vérificateur que la clé publique utilisée lors de la vérification correspond bien à l'auteur du texte signé

Votre réponse est correcte.

La réponse correcte est :
Une entropie élevée de la source qui génère les textes à signer

Question **16**

Correct

Note de 1,00 sur 1,00

Laquelle des options suivantes n'est pas une méthode d'authentification par mot de passe à usage unique (en anglais One-Time Password ou OTP)

- a. L'usager doit taper le contenu d'un captcha qui apparaît sur la page Web d'authentification et change à chaque fois ✔
- b. Le jeton d'authentification de type porte-clé génère un code à 4 chiffres valable pour une minute que l'utilisateur rentre sur la page Web d'authentification sur son laptop
- c. Le serveur envoie un code de 4 chiffres par SMS au numéro de téléphone cellulaire de l'usager enregistré pour l'usager concerné
- d. Le téléphone mobile du client génère un code à 6 chiffres valable pour une minute qui est envoyé au serveur d'authentification sur demande de l'usager

Votre réponse est correcte.

La réponse correcte est :
L'usager doit taper le contenu d'un captcha qui apparaît sur la page Web d'authentification et change à chaque fois

Question **17**

Correct

Note de 1,00 sur 1,00

Nous avons mentionné dans le cours que l'étape la plus importante du processus de gestion des risques informatiques était l'Étape 5 « retour à l'Étape 1 ». Nous avons évoqué plusieurs raisons soulignant son importance et nécessité. Laquelle de celles-ci n'en est pas une :

- a. L'évolution des priorités et le modèle d'affaires de la compagnie peuvent changer la probabilité et l'impact des différentes menaces
- b. Sans une réévaluation constante des risques en informatiques, il serait impossible aux compagnies de services spécialisées en sécurité informatique, qui sont un élément clé de la gestion de ce type de risque, de faire un profit raisonnable. ✔
- c. Les technologies et le mode d'utilisation des systèmes d'information changent avec le temps
- d. Les acteurs de menaces développent leur capacité avec le temps, que ce soit en termes de connaissance, de méthodes ou d'outils.

Votre réponse est correcte.

La réponse correcte est :
Sans une réévaluation constante des risques en informatiques, il serait impossible aux compagnies de services spécialisées en sécurité informatique, qui sont un élément clé de la gestion de ce type de risque, de faire un profit raisonnable.

Commentaire :

Question **18**

Correct

Note de 1,00 sur 1,00

Laquelle de ces affirmations est vraie :

- a. La technique par reconnaissance l'iris peut être utilisée pour authentifier un utilisateur jusqu'à 10 mètres de distance
- b. La technologie par reconnaissance du visage est fiable à 100%
- c. La technologie par reconnaissance rétinienne est la technologie biométrique la plus difficile à contrefaire ✔
- d. La technologie de lecture d'empreintes digitales ne peut pas être contrefaite

Votre réponse est correcte.

La réponse correcte est :
La technologie par reconnaissance rétinienne est la technologie biométrique la plus difficile à contrefaire

Question **19**

Correct

Note de 1,00 sur 1,00

La technologie par reconnaissance de l'iris repose sur 266 caractéristiques. La probabilité de similitude est extrêmement faible : 1/(10^78). Cela correspond à la probabilité de trouver du premier coup un mot de passe alphanumérique (composé de caractères minuscules a-z, et de chiffres 0-9) d'une longueur de :

- a. Environ 30 caractères
- b. 78 caractères
- c. Environ 50 caractères ✔
- d. Environ 100 caractères

Votre réponse est correcte.

Il y a 36 choix possibles pour chaque caractère du mot de passe (26 lettres et 10 chiffres).

Soit n la longueur du mot de passe.

Pour trouver n il suffit de résoudre l'équation 36^n = 10^78

Soit log36 (36^n) = log36 (10^78)

C'est-à-dire n = log36(10^78) = 78 log36(10) = 78 * 0,642 = 50

La réponse correcte est :
Environ 50 caractères

Question **20**

Terminer

Note de 2,00 sur 2,00

(Explication de la question précédente)

La technologie par reconnaissance de l'iris repose sur 266 caractéristiques. La probabilité de similitude est extrêmement faible : 1/(10^78).

Expliquez comment vous avez obtenu la réponse à la question précédente.

Une probabilité de 1/(10^78) indique qu'il existe 10^78 combinaisons différentes. Il faut donc trouver quelle longueur de mot de passe donne 10^78 combinaisons possibles. Il y a 36 symboles différents possibles (26 alphabet en miniscule + 10 chiffres). Donc 36^n combinaisons où n est la longueur du mot de passe. Nous cherchons donc 36^n=10^78. Il suffit de faire le log à base 36 des deux côtés pour trouver n. log(10^78)/log(36)=x = 50.11879...

Commentaire :

Question **21**

Correct

Note de 1,00 sur 1,00

Votre mot de passe est une « phrase » de passe composé de quatre mots du français courant, choisis au hasard dans un dictionnaire de 4000 mots.) Si vous deviez choisir un mot de passe composé de caractères alphabétiques (lettres minuscules a-z) et des chiffres 0 et 1, quel devrait être la longueur de ce mot de passe pour une sécurité équivalente ?

- a. Environ 12 caractères
- b. Environ 8 caractères
- c. Environ 10 caractères ✔
- d. Environ 6 caractères

Votre réponse est correcte.

On calcule d'abord l'entropie d'une source aléatoire qui tire un caractère dans l'alphabet (a-z et 0-1), soit 28 choix possibles : log2(28) = 4.81 bits.

Pour trouver la longueur du mot de passe, il suffit de diviser 48 (l'entropie de la phrase de passe constituée de 4 mots tirés dans un dictionnaire de 4000 mots) par 4,81.

On obtient un mot de passe d'une longueur d'environ 10 caractères.

La réponse correcte est :
Environ 10 caractères

Question **22**

Terminer

Note de 2,00 sur 2,00

(Explication de la question précédente)

Votre mot de passe est une « phrase » de passe composé de quatre mots du français courant, choisis au hasard dans un dictionnaire de 4000 mots.) Si vous deviez choisir un mot de passe composé de caractères alphabétiques (lettres minuscules a-z) et des chiffres 0 et 1, quel devrait être la longueur de ce mot de passe pour une sécurité équivalente ?

Expliquez comment vous avez obtenu la réponse à la question précédente.

Une phrase de passe de 4 mots d'un dictionnaire de 4000 mots permet 4000^4 combinaisons différentes. Il faut donc trouver quelle longueur de mot de passe donne 4000^4 combinaisons possibles. Il y a 28 symboles différents possibles (26 alphabet en miniscule + les chiffres 1 et 0). Donc 28^n combinaisons où n est la longueur du mot de passe. Nous cherchons donc 28^n=4000^4. Il suffit de faire le log à base 28 des deux côtés pour trouver n. log(4000^4)/log(28)=x = 9.95623...

Commentaire :

Question **23**

Terminer

Non noté

L'utilisation d'une méthode d'authentification avec mot de passe à usage unique (« one-time password » ou OTP en anglais) basée sur un secret partagé réduit le risque de compromission des comptes usagers dans le cas où la base de données d'usager est piratée.

Sélectionnez une réponse :

- Vrai
- Faux

La réponse correcte est « Faux ».

Question **24**

Terminer

Non noté

(Explication de la question précédente)

L'utilisation d'une méthode d'authentification avec mot de passe à usage unique (« one-time password ») basée sur un secret partagé réduit le risque de compromission des comptes usagers dans le cas où la base de données d'usager est piratée.

Expliquez votre réponse.

Malgré le fait que la base de données d'usager est piratée, le mot de passe est à usage unique. Le pirate informatique n'aura donc pas accès aux comptes s'il n'a pas aussi réussi à mettre la main sur le dispositif générant les mots de passes(téléphone, clé SecurID, etc.). Il y a deux canals à compromettre plutôt qu'un.

Question **25**

Correct

Note de 1,00 sur 1,00

Vous êtes le chef de sécurité informatique dans une centrale nucléaire. Vos responsabilités (« scope ») couvrent autant les technologies d'information traditionnelles (bureautique, Web, email, etc.), que les systèmes informatisés de contrôle du réacteur nucléaire et les systèmes informatisés de contrôle des systèmes auxiliaires (refroidissement, génération d'électricité, système de lutte contre les incendies, sécurité physique, etc.). Lequel de ces aspects de la sécurité devraient être votre priorité :

- a. Motivation
- b. Rapidité
- c. Confidentialité
- d. Honnêteté
- e. Disponibilité ✔

Votre réponse est correcte.

La réponse correcte est :

Disponibilité

Question **26**

Terminer

Note de 2,00 sur 2,00

(Explication de la question précédente)

Vous êtes le chef de sécurité informatique dans une centrale nucléaire. Vos responsabilités (« scope ») couvrent autant les technologies d'information traditionnelles (bureautique, Web, email, etc.), que les systèmes informatisés de contrôle du réacteur nucléaire et les systèmes informatisés de contrôle des systèmes auxiliaires (refroidissement, génération d'électricité, système de lutte contre les incendies, sécurité physique, etc.). Lequel de ces aspects de la sécurité devraient être votre priorité :

Expliquez votre réponse

Afin d'assurer la sécurité dans une centrale nucléaire, deux aspects sont très importants, l'intégrité des systèmes afin qu'ils opérent de la bonne manière et la disponibilité afin qu'ils réagissent. Les réponses a,b,d ne font pas partie des aspects de la sécurité. La confidentialité n'est pas l'aspect prioritaire d'une centrale nucléaire. Dans ce cas-ci, il est donc évident que la disponibilité est primordial puisque les systèmes auxiliaires doivent être fonctionnels au moment où une demande leur est acheminé. Si le système de refroidissement ou le système de luttre contre les incendies ne réagit pas, il pourrait en résulter une catastrophe qui se compte en vie humaine.

Commentaire :

◄ Video cours 5 - 25 février - Authentification

Aller à…

Examen Intra Hiver 2021 (reprise) ►

Commencé le	jeudi 20 octobre 2022, 14:00
État	Terminé
Terminé le	jeudi 20 octobre 2022, 16:00
Temps mis	1 heure 59 min
Points	23,50/40,00
Note	**5,88** sur 10,00 (**58,75**%)

Question **1**

Correct

Note de 1,00 sur 1,00

On considère un mot de passe généré de la façon suivante :

La longueur du mot de passe est toujours de 10 caractères

Chaque caractère est une lettre (minuscules de « a » à « z » ou majuscules de « A » à « Z ») ou un chiffre de « 0 » à « 9 ».

On suppose que chaque caractère est tiré de façon parfaitement aléatoire.

Quelle est l'entropie de ce mot de passe ?

a. Environ 5,7 bits

b. Environ 4,7 bits

c. Environ 57 bits

d. Environ 47 bits

e. Environ 60 bits ✔

f. Environ 6 bits

Votre réponse est correcte.

Réponse :

Entropie d'un caractère du mot de passe :

Log2(62) = 5,954

Entropie du mot de passe (10 caractères, source markovienne)

10 * 5,954 = 59,54

La réponse correcte est :
Environ 60 bits

Question **2**

Correct

Note de 1,00 sur 1,00

Dans la question précédente, les meilleures chances de casser le mot de passe sont de réaliser une attaque par dictionnaire.

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **3**

Correct

Note de 1,00 sur 1,00

Comme dans la question précédente, on considère un mot de passe généré de la façon suivante :

La longueur du mot de passe est toujours de 10 caractères

Chaque caractère est une lettre (minuscules de « a » à « z » ou majuscules de « A » à « Z ») ou un chiffre de « 0 » à « 9 ».

On suppose que chaque caractère est tiré de façon parfaitement aléatoire.

L'attaquant sait comment sont générés les mots de passe.

L'attaquant décide de réaliser une attaque par force brute.

L'attaquant peut tester 1 000 000 de mots de passe à la seconde.

On suppose qu'une année correspond à 365 jours.

Combien de temps est nécessaire pour que l'attaquant ait 100% de chance de casser le mot de passe ?

a. Environ 4 584 années

b. Environ 4,5 années

c. Environ 9 714 110 années

d. Environ 26 614 années ✔

Votre réponse est correcte.

Réponse :

Nombre de mots de passe possibles :

62^10 = 839 299 365 868 340 224

Nombre de secondes dans une année :

60 * 60 * 24 * 365 = 31 536 000

Nombre de mots de passe testés dans une année :

1 000 000 * 31 536 000 = 31 536 000 000 000

Temps nécessaire pour avoir 100% de chance de trouver le mot de passe :

839 299 365 868 340 224 / 31 536 000 000 000 = 26 614 années

La réponse correcte est :
Environ 26 614 années

Question **4**

Incorrect

Note de 0,00 sur 1,00

On considère qu'un mot de passe est « faible » si ce mot de passe peut être cassé en moins de 30 jours par force brute.

On suppose que le mot de passe est généré comme dans la question précédente.

L'attaquant sait comment sont générés les mots de passe.

L'attaquant décide de réaliser une attaque par force brute.

L'attaquant peut tester 1 000 000 de mots de passe à la seconde.

On suppose que les capacités de tester des mots de passe vont suivre la loi de Moore, c'est-à-dire le nombre de mots de passe que l'attaquant peut tester en une seconde va doubler tous les 18 mois.

Au bout de combien d'années le mot de passe considéré dans la question précédente va devenir faible ?

a. Environ 23,7 années ✖

b. Environ 27,5 années

c. Environ 40,2 années

d. Environ 8,7 années

Votre réponse est incorrecte.

Réponse :

Nombre N1 de jours nécessaires aujourd'hui pour casser le mot de passe :

N1 = 839 299 365 868 340 224 / 86 400 000 000 = 9 714 113 jours

Au bout de n années, les capacités de l'attaquant auront été multipliées par 2^(n/1,5)

On cherche donc n tel que :

N1 / 2^(n/1,5) < 30

Soit :

N1 / 30 < 2^(n/1,5)

C'est-à-dire :

Log2(N1/30) < n/1,5

Donc n > 1,5 * Log2(9 714 113 / 30) = 1,5 * 18,30 = 27,45

Donc n = 27,5 années

La réponse correcte est :
Environ 27,5 années

Question **5**

Terminé

Note de 0,50 sur 2,00

Justifier par le calcul votre réponse à la question précédente

nombre de second par annee est : 2^25

nombre d'essai par second est = 2^20

nombre d'essai par annee est : 2^45

les mots de pass a essayé sont : 2^60

il nous faut pour tout essayer 2^60/2^45 = 2^15 ans = 32000ans

on utilisant la loi de moore :

15 * 1.5 = 22.5 ans pour casser le mot de passe

Commentaire :
Erreur de calcul --> 30 jours pas un an

Question **6**

Correct

Note de 1,00 sur 1,00

On considère un mot de passe généré de la façon suivante :

La longueur du mot de passe est toujours de 8 caractères.

Les 7 premiers caractères sont des lettres (minuscules de « a » à « z » ou majuscules de « A » à « Z »)

Le huitième caractère est une lettre (minuscules de « a » à « z » ou majuscules de « A » à « Z ») ou un chiffre de « 1 » à « 9 »

L'attaquant sait comment sont générés les mots de passe.

L'attaquant décide de réaliser une attaque par force brute.

L'attaquant peut tester 1 000 000 de mots de passe à la seconde.

On suppose qu'une année correspond à 365 jours.

Combien de temps est nécessaire pour que l'attaquant ait 50% de chance de casser le mot de passe ?

a. Environ 1,69 année

b. Environ 2 ans

c. Environ 3,46 années

d. Environ 1 an ✔

Votre réponse est correcte.

Réponse :

Nombre de mots de passe possibles :

52^7 * 62 = 63 740 445 556 736

Nombre de secondes dans une année :

60 * 60 * 24 * 365 = 31 536 000

Nombre de mots de passe testés dans une année :

1 000 000 * 31 536 000 = 31 536 000 000 000

Temps nécessaire pour avoir 50% de chance de trouver le mot de passe :

0,5 * 63 740 445 556 736 / 31 536 000 000 000 = 1,01 année

La réponse correcte est :
Environ 1 an

Question **7**

Correct

Note de 1,00 sur 1,00

On considère un mot de passe généré de la façon suivante :

La longueur du mot de passe est toujours de 8 caractères

Les 7 premiers caractères sont des lettres (minuscules de « a » à « z » ou majuscules de « A » à « Z »)

Le huitième caractère est une lettre (minuscules de « a » à « z » ou majuscules de « A » à « Z ») ou un chiffre de « 1 » à « 9 »

Il y a 80% de chance que le huitième caractère soit un chiffre et seulement 20% de chance que ce soit une lettre.

L'attaquant sait comment sont générés les mots de passe.

L'attaquant décide de réaliser une attaque par force brute.

L'attaquant peut tester 1 000 000 de mots de passe à la seconde.

Combien de temps est nécessaire pour que l'attaquant ait 50% de chance de casser le mot de passe ?

- a. Environ 59,5 jours
- b. Environ 365 jours
- c. Environ 119 jours
- d. Environ 74,37 jours ✔

Votre réponse est correcte.

Réponse :

Nombre de mots de passe testés dans une journée :

1 000 000 * 60 * 60 * 24 = 86 400 000 000

Nombre de mots de passe composés de 7 lettres et d'un chiffre en huitième position :

52^7 * 10 = 10 280 717 025 280

En testant ces mots de passe, l'attaquant a 80% de chance de trouver le bon mot de passe.

Nombre de jours nécessaires pour avoir 50% de trouver le bon mot de passe :

(50 / 80) * (10 280 717 025 280 / 86 400 000 000) = 74,37 jours

La réponse correcte est :
Environ 74,37 jours

Question **8**

Incorrect

Note de 0,00 sur 1,00

On considère un mot de passe généré de la façon suivante :

La longueur du mot de passe est toujours de 8 caractères

Les 7 premiers caractères sont des lettres (minuscules de « a » à « z » ou majuscules de « A » à « Z »)

Le huitième caractère est une lettre (minuscules de « a » à « z » ou majuscules de « A » à « Z ») ou un chiffre de « 1 » à « 9 »

L'attaquant sait comment sont générés les mots de passe.

L'attaquant décide de réaliser une attaque par dictionnaire.

Le dictionnaire contient 1000 mots de 7 lettres composés de minuscules.

Le dictionnaire contient 2000 mots de 8 lettres composés de minuscules.

Combien de mots de passe l'attaquant doit-il tester pour réaliser cette attaque par dictionnaire ?

- a. 3 000 ✖
- b. 768 000
- c. 3 840 000
- d. 512 000
- e. 1 792 000
- f. 12 000

Votre réponse est incorrecte.

Réponse :

Avec un mot de 7 lettres composé de minuscules, on peut forger 2^7 = 128 mots de 7 lettres composés de minuscules ou de majuscules.

Avec un mot de 8 lettres composé de minuscules, on peut forger 2^8 = 256 mots de 8 lettres composés de minuscules ou de majuscules.

Nombre de mots 8 lettres composés de minuscules ou de majuscules à tester :

2000 * 256 = 512 000

Nombre de mots 8 lettres à tester, composés de 7 lettres minuscules ou majuscules et d'un chiffre en huitième position :

1000 * 128 * 10 = 1 280 000

Nombre total de mots de passe à tester :

512 000 + 1 280 000 = 1 792 000 mots de passe

La réponse correcte est :
1 792 000

Question **9**

Correct

Note de 1,00 sur 1,00

On considère une phrase de passe générée de la façon suivante :

La phrase de passe est composée de 4 mots.

Chaque mot est tiré au hasard dans un dictionnaire de 5000 mots composés de minuscules.

L'attaquant sait comment sont générées les phrases de passe.

L'attaquant a accès au dictionnaire utilisé pour générer les phrases de passe.

L'attaquant décide de réaliser une attaque par force brute.

L'attaquant peut tester 1 000 000 de phrases de passe à la seconde.

On suppose qu'une année correspond à 365 jours.

Combien de temps est nécessaire pour que l'attaquant ait 100% de chance de casser la phrase de passe ?

- a. 19,82 années ✔
- b. 0,005 seconde
- c. 25 secondes
- d. 7233,8 années

Votre réponse est correcte.

Réponse :

Nombre de phrases de passe à tester :

5000 ^4 = 625 000 000 000 000

Nombre de mots de passe testés dans une année :

1 000 000 * 31 536 000 = 31 536 000 000 000

Temps nécessaire pour avoir 100% de chance de trouver le mot de passe :

625 000 000 000 000 / 31 536 000 000 000 = 19,82 années

La réponse correcte est :
19,82 années

Question **10**

Correct

Note de 1,00 sur 1,00

On considère une phrase de passe générée de la façon suivante :

La phrase de passe est composé de 4 mots.

Chaque mot est tiré au hasard dans un dictionnaire de 5000 mots composés de minuscules.

Mais chaque mot composant finalement la phrase de passe peut être composé d'une minuscule ou d'une majuscule en première position. Les autres lettres restent des minuscules. Par exemple, si le mot « canada » est tiré au hasard, alors le mot final peut-être « Canada » ou « canada ».

L'attaquant sait comment sont générées les phrases de passe.

L'attaquant a accès au dictionnaire utilisé pour générer les phrases de passe.

L'attaquant décide de réaliser une attaque par force brute.

Si l'on compare avec la question précédente, combien de temps est nécessaire pour que l'attaquant ait 100% de chance de casser la phrase de passe ?

- a. 16 fois plus de temps ✔
- b. 4 fois plus de temps
- c. 2 fois plus de temps
- d. 10 fois plus de temps

Votre réponse est correcte.

Réponse :

Pour chaque mot du dictionnaire, il est possible de générer deux mots.

Avec 5000 mots dans le dictionnaire, il faut tester 10000 mots.

Pour une phrase de passe composée de 4 mots, il faut donc tester 10000^4 phrases de passe.

Si l'on compare avec la question précédente, il fallait tester 5000^4 phrases de passe.

L'attaquant aura donc besoin de :

10000 ^4 / 5000 ^4 = 2^4 = 16 fois plus de temps

La réponse correcte est :
16 fois plus de temps

Question **11**

Incorrect

Note de 0,00 sur 2,00

On considère une source S qui génère des chaînes de bits (0 ou 1) de la façon suivante :

Si la position du bit dans la chaîne est impaire, alors il y a 50% de chance que le bit soir un 0 et 50% de chance que ce soit un 1.

Si la position du bit dans la chaîne est paire, alors : (1) si le bit précédent dans la chaîne est un 0, il y a 30% de chance que le bit soit un 0 et 70% de chance que le bit soit un 1 et (2) si le bit précédent dans la chaîne est un 1, il y a 30% de chance que le bit soit un 1 et 70% de chance que le bit soit un 0.

Quelle est l'entropie caractère par caractère de la source S ?

- a. 1 bit
- b. 0,5 bit
- c. 0,74 bit
- d. 0,7 bit ✖

Votre réponse est incorrecte.

Réponse question 11 :

Il s'agit de calculer la fréquence d'apparition des 0 et des 1 dans la chaîne générée par la source S.

La séquence « 00 » apparait dans 0,5 * 0,3 = 15% des cas.

La séquence « 01 » apparait dans 0,5 * 0,7 = 35% des cas.

La séquence « 10 » apparait dans 0,5 * 0,7 = 35% des cas.

La séquence « 11 » apparait dans 0,5 * 0,3 = 15% des cas.

La probabilité d'apparition d'un 0 dans la chaîne est donc de :

(0,15 * 2 + 0,35 + 0,35) / 2 = 0,5

Et la probabilité d'apparition d'un 1 dans la chaîne est donc également de 0,5.

L'entropie caractère par caractère de la source S est donc de 1 bit.

La réponse correcte est :
1 bit

Question **12**

Correct

Note de 1,00 sur 1,00

Suite de la question précédente.

La source S est markovienne.

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **13**

Incorrect

Note de 0,00 sur 1,00

On considère la source S^2 identique à la source S mais qui génère des blocs de 2 bits (digrammes).

La source S^2 est-elle markovienne ?

Veuillez choisir une réponse.

- Vrai
- Faux ✖

La réponse correcte est « Vrai ».

Question **14**

Non répondue

Noté sur 1,00

On considère la source S^2 identique à la question précédente.

Quelle est l'entropie de la source S^2 ?

a. 1 bit

b. 2 bits

c. 1,47

d. 1,82

Votre réponse est incorrecte.

Réponse :

L'alphabet de la source S^2 est {00, 01, 10, 11}

On a :

P(S^2 = « 00 ») = 0,15

P(S^2 = « 01 ») = 0,35

P(S^2 = « 10 ») = 0,35

P(S^2 = « 11 ») = 0,15

En appliquant la formule de Shannon, on a :

H(S^2) = 0,15 Log2(1/0,15) + 0,35 Log2(1/0,35) + 0,35 Log2(1/0,35) + 0,15 Log2(1/0,15)

Donc H(S^2) = - 0,3 Log2(0,15) – 0,7 Log2(0,35) = 0.30 x 2.7369 + 0.70 x 1.51457 = 1,88

Petite faute de frappe dans la réponse mais la réponse acceptée est 1,82

La réponse correcte est :
1,82

Question **15**

Non répondue

Noté sur 2,00

Justifier par le calcul votre réponse à la question précédente

Question **16**

Incorrect

Note de 0,00 sur 1,00

On considère la source S^2 identique à la question précédente.

Quelle est l'entropie du langage associé à la source S ?

a. Egale à l'entropie caractère par caractère de la source S

b. Egale à l'entropie de la source S^2

c. Egale à la moitié de l'entropie de la source S^2

d. Aucune de ces réponses ✖

Votre réponse est incorrecte.

Réponse :

On a H_L(S) = lim{b --> infini} (H(S^b) / b)

Si b = 2n (b est pair) alors H(S^2n) = n H(S^2) car S^2 est markovienne.

H_L(S) = lim{2n --> infini} (n H(S^2) / 2n) = H(S^2) / 2

Si b = 2n + 1 (b est impair) alors H(S^b) = n H(S^2) + 1

H_L(S) = lim{2n+1 --> infini} ((n H(S^2) + 1) / (2n + 1))

= lim (2n+1 --> infini} (n H(S^2) / (2n + 1)) + lim (2n+1 infini} (1 / (2n + 1))

Donc H_L(S) = H(S^2) / 2 + 0 = H(S^2) / 2

La réponse est donc : H_L(S) = H(S^2) / 2

La réponse correcte est :
Egale à la moitié de l'entropie de la source S^2

Question **17**

Correct

Note de 1,00 sur 1,00

Alice a envoyé un message confidentiel à Bob en utilisant le chiffrement RSA

Quelle opération doit faire Bob pour accéder au message ?

a. Déchiffrer avec la clé publique d'Alice

b. Déchiffrer avec la clé privée de Bob ✔

c. Déchiffrer avec la clé publique de Bob

d. Déchiffrer avec la clé privée d'Alice

Votre réponse est correcte.

La réponse correcte est :
Déchiffrer avec la clé privée de Bob

Question **18**

Correct

Note de 1,00 sur 1,00

Alice a signé un message en utilisant le chiffrement RSA et l'a envoyé à Bob.

Quelle action doit faire Bob pour vérifier la signature d'Alice ?

a. Déchiffrer avec la clé privée d'Alice

b. Déchiffrer avec la clé privée de Bob

c. Déchiffrer avec la clé publique de Bob

d. Déchiffrer avec la clé publique d'Alice ✔

Votre réponse est correcte.

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

Question **19**

Partiellement correct

Note de 1,00 sur 4,00

Nous sommes en 2040 et le chiffrement AES avec une clé de 128 bits est devenu obsolète.

Il est désormais recommandé d'utiliser AES avec une clé de 256 bits.

On considère un document d et une clé AES k1 de 128 bits.

Soit D le résultat du chiffrement de d avec la clé k1.

Soit k2 une clé AES de 128 bits.

Soit k3 une clé AES de 256 bits.

On suppose que l'on dispose de l'espace mémoire nécessaire pour faire une attaque « Meet in The Middle ».

Evaluer les opérations suivantes en termes de force de chiffrement :

Déchiffrer D avec k2 et chiffrer avec k1	Equivalent à une clé de 129 bits	✗
Déchiffrer D avec k1 et chiffrer avec k3	Equivalent à une clé de 129 bits	✗
Chiffrer D avec k2 et chiffrer avec k1	Equivalent à une clé de 129 bits	✗
Chiffrer D avec k3 et chiffrer avec k1	Equivalent à une clé de 129 bits	✗
Chiffrer D avec k2	Equivalent à une clé de 128 bits	✗
Chiffrer deux fois D avec k2	Equivalent à une clé de 128 bits	✗
Chiffrer D avec k3	Equivalent à une clé de 256 bits	✓
Chiffrer D avec k1	Equivalent à une clé de 128 bits	✓

Votre réponse est partiellement correcte.

Vous en avez sélectionné correctement 2.
La réponse correcte est :
Déchiffrer D avec k2 et chiffrer avec k1 → Equivalent à une clé de 256 bits,

Déchiffrer D avec k1 et chiffrer avec k3 → Equivalent à une clé de 256 bits,

Chiffrer D avec k2 et chiffrer avec k1 → Equivalent à une clé de 256 bits,

Chiffrer D avec k3 et chiffrer avec k1 → Equivalent à une clé de 392 bits,

Chiffrer D avec k2 → Equivalent à une clé de 129 bits,

Chiffrer deux fois D avec k2 → Equivalent à une clé de 129 bits,

Chiffrer D avec k3 → Equivalent à une clé de 256 bits,

Chiffrer D avec k1 → Equivalent à une clé de 128 bits

Question **20**

Correct

Note de 1,00 sur 1,00

Nous sommes en 2050 et le premier ordinateur quantique avec plusieurs milliers de Qbits a été commercialisé.

On considère un document chiffré avec une clé de chiffrement AES de 256 bits.

Quelle opération est adaptée pour faire face à la situation :

a. Déchiffrer le document et le chiffrer avec une clé AES de 512 bits ✔

b. Déchiffrer le document et le chiffrer avec une clé RSA de 4096 bits

c. Le chiffrement AES est désormais obsolète. Il faut le remplacer par un algorithme de chiffrement post-quantique.

d. On n'a rien à faire. L'ordinateur quantique n'a pas d'effet sur le chiffrement AES

Votre réponse est correcte.

La réponse correcte est :
Déchiffrer le document et le chiffrer avec une clé AES de 512 bits

Question **21**

Incorrect

Note de 0,00 sur 1,00

On vous demande quelle est la forme d'authentification la plus faible. Que répondriez-vous ?

a. Les scans de la rétine

b. La reconnaissance faciale ✖

c. Les mots de passe

Votre réponse est incorrecte.

La réponse correcte est :
Les mots de passe

Question **22**

Correct

Note de 1,00 sur 1,00

Soit FAR = FA ÷ TA, où

FAR = taux de fausses acceptations (False Acceptance Ratio)

FA = Nombre de fausses acceptations (Number of False Acceptances)

TA = Nombre total de tentatives (Total Number of Attempts)

Votre organisation a décidé d'utiliser un système biométrique pour authentifier les utilisateurs. Si le FAR est élevé, que se passe-t-il ?

a. Les utilisateurs légitimes se voient refuser l'accès aux ressources de l'organisation.

b. Les utilisateurs légitimes ont accès aux ressources de l'organisation.

c. Les utilisateurs illégitimes se voient refuser l'accès aux ressources de l'organisation.

d. Les utilisateurs illégitimes ont accès aux ressources de l'organisation. ✔

Votre réponse est correcte.

La réponse correcte est :
Les utilisateurs illégitimes ont accès aux ressources de l'organisation.

Question **23**

Correct

Note de 1,00 sur 1,00

Lequel des éléments suivants est la forme la plus simple et la plus courante d'attaque de hashés de mots de passe hors ligne utilisée pour récupérer des mots de passe non sécurisés ?

a. Dictionnaire ✔

b. Homme du milieu

c. Clé USB

d. Force brute

Votre réponse est correcte.

La réponse correcte est :
Dictionnaire

Question **24**

Correct

Note de 2,00 sur 2,00

Lequel des énoncés suivants décrit le mieux l'authentification par défi/réponse ?

a. C'est un protocole d'authentification dans lequel une valeur de sel est présentée à l'utilisateur, qui renvoie ensuite un hachage MD5 basé sur cette valeur de sel.

b. Il s'agit d'un protocole d'authentification dans lequel un système de tickets est utilisé pour valider les droits de l'utilisateur à accéder aux ressources et aux services.

c. Il s'agit d'un protocole d'authentification dans lequel une chaîne de valeurs générée de manière aléatoire est présentée à l'utilisateur, qui renvoie ensuite un nombre calculé sur la base de ces valeurs aléatoires. ✔

d. C'est un protocole d'authentification dans lequel le nom d'utilisateur et le mot de passe sont transmis au serveur en utilisant un protocole appelé CHAP (Challenge-Handshake Authentication Protocol)

Votre réponse est correcte.

La réponse correcte est :
Il s'agit d'un protocole d'authentification dans lequel une chaîne de valeurs générée de manière aléatoire est présentée à l'utilisateur, qui renvoie ensuite un nombre calculé sur la base de ces valeurs aléatoires.

Question **25**

Correct

Note de 1,00 sur 1,00

Quelle est la meilleure façon de stocker les mots de passe ?

a. Au moyen d'une signature numérique

b. Dans un fichier chiffré à sens unique ✔

c. En utilisant un chiffrement asymétrique

d. En utilisant un chiffrement symétrique

Votre réponse est correcte.

La réponse correcte est :
Dans un fichier chiffré à sens unique

Question **26**

Correct

Note de 1,00 sur 1,00

Laquelle des propositions suivantes ne correspond pas à une authentification double facteur ?

a. L'énoncé d'une phrase secrète et la présentation d'une carte d'identité

b. La présentation à la fois de la paume de la main et des empreintes digitales ✔

c. Présentation de son visage à une caméra et la pause de son poignet à un lecteur de la puce qui y a été implantée sous la peau

d. La saisie d'un mot de passe pris dans un dictionnaire Yiddish et la captation du rythme de frappe sur un clavier

Votre réponse est correcte.

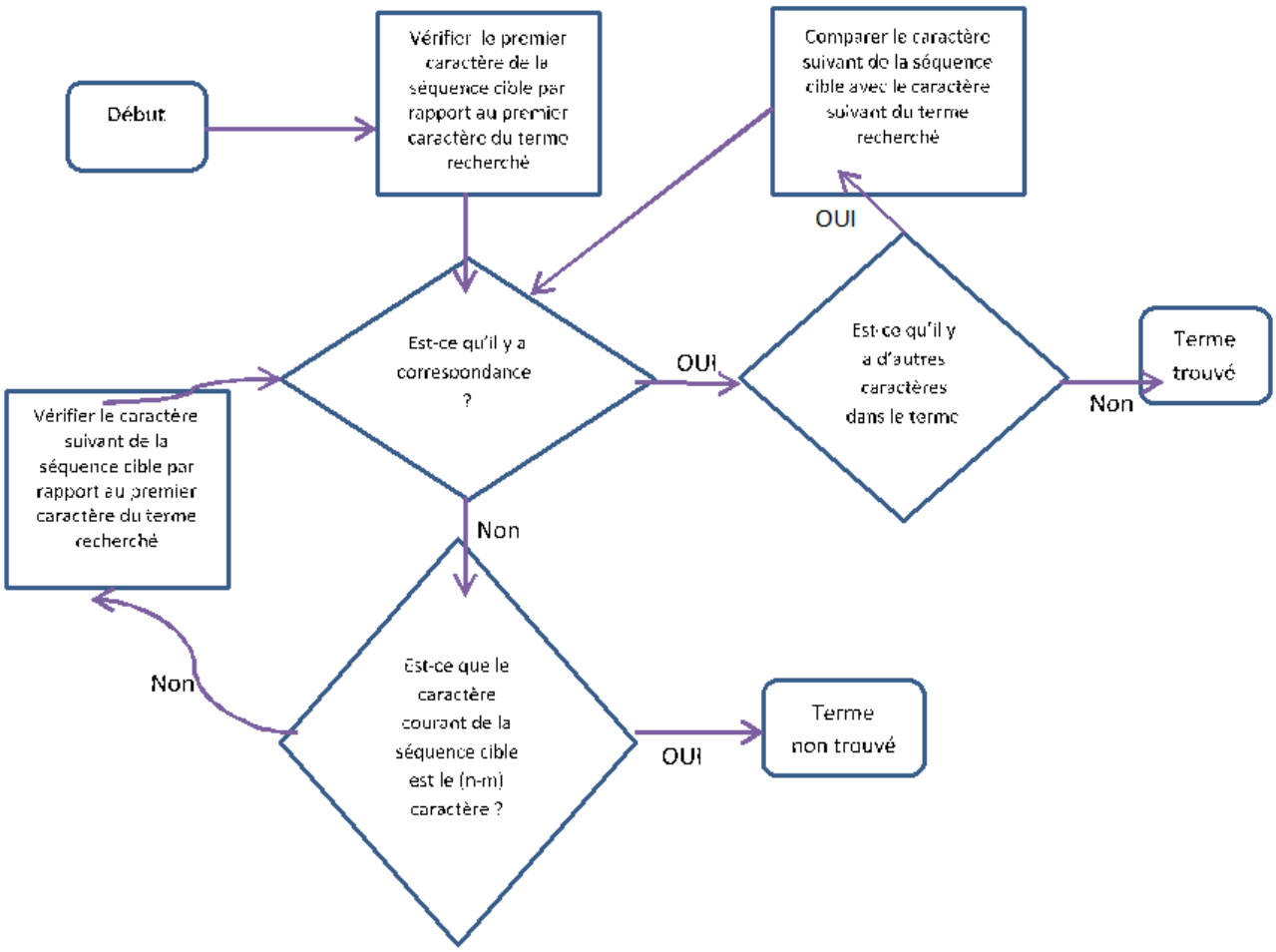
La réponse correcte est :
La présentation à la fois de la paume de la main et des empreintes digitales

Question **27**

Incorrect

Note de 0,00 sur 1,00

Soit une esquisse d'un algorithme schématisé par la figure suivante :



S'agit-il d'un algorithme d'attaque par :

- a. Ingénierie sociale
- b. Brute force
- c. Blocs ✖
- d. Dictionnaire

Votre réponse est incorrecte.

La réponse correcte est :
Brute force

Question **28**

Correct

Note de 1,00 sur 1,00

Au cours des mois de mars et d'avril 2000, un ancien prestataire technique de la station d'épuration de Maroochy en Australie a pris le contrôle des systèmes de l'usine à des fins malveillantes, après que sa demande d'emploi ait été refusée. Il aurait ainsi détourné l'activité de plusieurs pompes en envoyant de fausses commandes. L'une des pompes aurait alors cessé de fonctionner, provoquant le déversement d'eaux usées dans les fonds marins, l'empoisonnement de la faune et de la flore locales, et la propagation d'odeurs nauséabondes aux alentours. Quel paramètre de la probabilité d'occurrence de cette attaque a facilité la tâche de l'attaquant :

a. Vulnérabilité

b. Capacité

c. Opportunité ✔

d. Motivation

Votre réponse est correcte.

La réponse correcte est :
Opportunité

Question **29**

Correct

Note de 1,00 sur 1,00

Paula utilise un VPN pour établir une connexion chiffrée pour accéder à ses applications lorsqu'elle utilise le réseau public de l'aéroport.

Est-ce qu'il s'agit :

a. D'une contremesure ? ✔

b. D'une vulnérabilité ?

c. D'un risque ?

d. D'une menace ?

Votre réponse est correcte.

La réponse correcte est :
D'une contremesure ?

Question **30**

Correct

Note de 1,00 sur 1,00

Quelle est l'erreur dans l'analyse de risque suivante?

Scénario	Capacité	Opportunité	Motivation	Probabilité	Impact	Risque
A) Un administrateur de sécurité réalise une attaque en rançon logiciel ciblant une grande banque	3	2	3	2.67	4	12
B) Un cybercriminel réalise une attaque en rançon logiciel ciblant une grande banque	4	2	3	3	4	12

a. Aucune des propositions n'est correcte

b. Le facteur motivation dans B est trop élevé

c. Le risque de A ne prend pas en compte la probabilité et l'impact ✔

d. Le facteur capacité dans B est trop haut

e. L'impact dans B est trop élevé

f. Le risque de B est trop élevé

Votre réponse est correcte.

La réponse correcte est :
Le risque de A ne prend pas en compte la probabilité et l'impact

Question **31**

Correct

Note de 1,00 sur 1,00

EasyChair est un système de gestion Web d'articles en ligne. Il est utilisé pour gérer des conférences nationales ou internationales. Pour les chercheurs, ce système leur permet de soumettre leurs articles de recherche à une ou plusieurs conférences. Il leur offre ainsi la possibilité de modifier les contenus de leurs articles ainsi que les informations relatives à leurs articles soumis, de recevoir des commentaires du comité scientifique et de recevoir la notification de l'acceptation ou le rejet de leurs articles. Les articles soumis sont des travaux originaux non publiés par ailleurs. Le contenu du site pour une conférence donnée sur easychair, est géré par le président du comité scientifique de la conférence. Ce comité scientifique est composé de membres invités par le président. Le président affecte les articles aux différents membres et leur donne accès en lecture à ces articles et en écriture sur le site pour saisir leurs notes, leurs commentaires et leurs décisions (accepté, rejeté). Chaque article est relu par 3 membres du comité scientifiques. Les membres du comité scientifiques peuvent eux-mêmes soumettre leurs propres articles.

On vous demande de sélectionner la proposition la plus vraisemblable pour l'agent de la menace et le scénario correspondant suivants.

Scénario A. le président du comité scientifique, accepte des articles alors que les membres du comité scientifique les ont pour la majorité rejetés.

a.

Impact	Capacité	Motivation	opportunité	probabilité	Risque
4	2	1	2	1,66	6,64

b. ✔

Impact	Capacité	Motivation	opportunité	probabilité	Risque
4	2	1	4	2,33	9,33

Votre réponse est correcte.

La réponse correcte est :

Impact	Capacité	Motivation	opportunité	probabilité	Risque
4	2	1	4	2,33	9,33

Question **32**

Correct

Note de 1,00 sur 1,00

Suite de la question précédente.

On vous demande de sélectionner la proposition la plus vraisemblable pour l'agent de la menace et le scénario correspondant suivants.

Scénario B. un membre du comité scientifique, s'affecte deux articles alors qu'il est en conflit d'intérêt avec les auteurs sans l'avoir déclaré. Son intention est soit de les favoriser au niveau de la décision finale soit pour orienter la décision vers un rejet.

a.

Impact	Capacité	Motivation	opportunité	probabilité	Risque
2	2	4	2	2,66	5,33

b.

Impact	Capacité	Motivation	opportunité	probabilité	Risque
4	2	4	2	2,66	10,66

Votre réponse est correcte.

La réponse correcte est :

Impact	Capacité	Motivation	opportunité	probabilité	Risque
2	2	4	2	2,66	5,33

Question **33**

Incorrect

Note de 0,00 sur 1,00

Suite de la question précédente.

On vous demande de sélectionner la proposition la plus vraisemblable pour l'agent de la menace et le scénario correspondant suivants.

Scénario C : l'utilisateur soumissionnaire d'un article change les évaluations de son article. Cet utilisateur est membre du comité scientifique.

a.

Impact	Capacité	Motivation	opportunité	probabilité	Risque
2	2	4	2	2,66	5,33

b.

Impact	Capacité	Motivation	opportunité	probabilité	Risque
1	1	4	2	2,33	2,33

Votre réponse est incorrecte.

La réponse correcte est :

Impact	Capacité	Motivation	opportunité	probabilité	Risque
1	1	4	2	2,33	2,33

◄ Cours Crypto 3 Capsule 7 Attaques - Principes Utilisation Crypto

Aller à...

Support-Séance7-Cours ►