Commencé le	jeudi 19 janvier 2023, 14:02
État	Terminé
Terminé le	jeudi 2 février 2023, 14:15
Temps mis	14 jours
Points	8,00/17,00
Note	**4,71** sur 10,00 (**47,06**%)

Question **1**

Correct

Note de 1,00 sur 1,00

Complétez la phrase, un scénario est l'exploitation _____ par un acteur pour obtenir un impact ?

Veuillez choisir une réponse.

- a. d'une vulnérabilité ✔
- b. d'un logiciel
- c. d'une personne
- d. d'une attaque

Votre réponse est correcte.

La réponse correcte est : d'une vulnérabilité

Question **2**

Correct

Note de 1,00 sur 1,00

Le risque informatique lié à un ordinateur déconnecté du réseau et enfermé dans un coffre-fort dont seul le propriétaire connait la combinaison est négligeable

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **3**

Incorrect

Note de 0,00 sur 1,00

Pour deux mesures de sécurité dont les coûts totaux de possession (incluant coût d'achat, coût d'opération, coûts d'installation, etc.) sont équivalents, il convient de choisir celle qui réduit le plus le risque résiduel

Veuillez choisir une réponse.

- Vrai ✖
- Faux

La réponse correcte est « Faux ».

Question **4**

Correct

Note de 1,00 sur 1,00

Une fois votre analyse de risque terminée, vous déterminez que le risque est trop élevé. Vous avez le choix entre trois contre-mesures. Sur quels critères allez-vous baser votre sélection ?

Veuillez choisir une réponse.

a. Le type de chiffrement, les coûts d'opération et le prix d'acquisition

b. Le prix d'acquisition, les coûts liés à l'opération et la réduction du risque ✔

c. Le fournisseur, le prix d'acquisition et le risque résiduel

d. Le fournisseur, le type de chiffrement et le bonus offert par la compagnie si vous sélectionnez leur solution

e. Les coûts liés à l'opération, la réduction du risque et le risque résiduel

Votre réponse est correcte.

La réponse correcte est : Le prix d'acquisition, les coûts liés à l'opération et la réduction du risque

Question **5**

Incorrect

Note de 0,00 sur 1,00

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

Veuillez choisir une réponse.

a. Le cout d'achat de la contremesure A est supérieur à celui de B et C

b. Votre assureur en risque informatique offre une réduction de prime d'assurance si vous choisissez d'installer C

c. Le responsable de sécurité informatique d'une autre compagnie similaire vous indique que les usagers de son entreprise se sont plaints du manque de convivialité et de la perte de temps engendrée par le déploiement de la contremesure B ✖

d. La contremesure C s'est avéré efficace lors de son introduction dans le marché de la sécurité informatique il y a une vingtaine d'années, et est aujourd'hui toujours très largement utilisée

Votre réponse est incorrecte.

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

Question **6**

Incorrect

Note de 0,00 sur 1,00

Lorsqu'un acteur de menace prend un cours universitaire en sécurité informatique et augmente sa connaissance dans le but de l'appliquer pour faire le mal, lequel des facteurs suivants de l'analyse de risque sera augmenté :

Veuillez choisir une réponse.

a. Capacité

b. Opportunité ✖

c. Compétence

d. Motivation

Votre réponse est incorrecte.

La réponse correcte est : Capacité

Question **7**

Correct

Note de 1,00 sur 1,00

Lequel de ces facteurs de l'analyse de risque en sécurité informatique un ingénieur informatique, consultant externe en sécurité informatique pour une grande entreprise, est le plus en mesure de pouvoir évaluer correctement :

Veuillez choisir une réponse.

a. Impact ✔

b. Capacité

c. Motivation

d. Cout d'opération

Votre réponse est correcte.

La réponse correcte est : Impact

Question **8**

Correct

Note de 1,00 sur 1,00

L'analyse de risque doit être incluse dans l'analyse d'un projet. Ainsi, les analyses de risques sont réalisées exclusivement dans la phase de planification d'un projet

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

Question **9**

Correct

Note de 1,00 sur 1,00

Lorsque j'active les options de chiffrement du disque dur, je viens de réduire le facteur « opportunité » de la probabilité qu'un pirate puisse violer la confidentialité des informations qui se trouvent sur mon portable.

Veuillez choisir une réponse.

Vrai ✔

Faux

La réponse correcte est « Vrai ».

Question **10**

Incorrect

Note de 0,00 sur 1,00

Bien qu'un malfaiteur connaisse très peu l'informatique, il est fort probable qu'il trouve un moyen d'attaquer votre système s'il a assez d'argent pour avoir accès à des « pirates informatiques à gage » prêts à faire n'importe quoi pour de l'argent. Lequel des éléments de l'analyse de risque devrait être suffisamment élevé pour refléter cette situation ?

Veuillez choisir une réponse.

a. Coût

b. Motivation ✖

c. Probabilité

d. Capacité

Votre réponse est incorrecte.

La réponse correcte est : Capacité

Question **11**

Incorrect

Note de 0,00 sur 1,00

Lorsqu'un acteur de menace soudoie un employé de la compagnie où se trouve sa cible, lequel des attributs suivants de l'analyse de risque est affecté :

Veuillez choisir une réponse.

a. Intégrité ✖

b. Capacité

c. Opportunité

d. Motivation

Votre réponse est incorrecte.

La réponse correcte est : Opportunité

Question **12**

Incorrect

Note de 0,00 sur 1,00

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

Scénario	Capacité	Opportunité	Motivation	Probabilité	Impact	Risque
A) Un cyber criminel exploite un débordement de mémoire tampon (buffer overflow) pour causer une explosion.	3	3	2	2.67	4	10.67
B) Un usager typique exploite un débordement de mémoire tampon (buffer overflow) pour causer une explosion.	4	3	2	3	4	12

Veuillez choisir une réponse.

a. Le risque de A est trop faible

b. L'impact dans B est trop haut

c. Le facteur motivation dans A est trop faible ✖

d. La probabilité dans B ne prend pas en compte l'impact

e. Le facteur capacité dans B est trop haut

Votre réponse est incorrecte.

La réponse correcte est : Le facteur capacité dans B est trop haut

Question **13**

Correct

Note de 1,00 sur 1,00

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

Menace	Capa-cité	Oppor-tunité	Moti-vation	Proba-bilité	Impact	Risque
A) Un criminel informatique commun s'installe dans un cyber café et intercepte 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.	3	3	2	2.67	4	10.67
B) Un criminel informatique commun infecte le serveur d'un site Web populaire et y installe du contenu malveillant qui infecte toutes les machines qui visitent le site avec un « keylogger », qui enregistre les mots de passe et carte de crédit taper sur les machines infectées, afin de faire de la fraude bancaire par Internet.	2	3	2	2.33	4	9.33

Veuillez choisir une réponse.

a. Le risque de A est trop faible

b. L'impact de B est trop haut

c. Le facteur opportunité dans A est trop haut ✔

d. La probabilité de B ne prend pas en compte l'impact

e. Le facteur capacité dans B est trop haut

Votre réponse est correcte.

La réponse correcte est : Le facteur opportunité dans A est trop haut

Question **14**

Correct

Note de 1,00 sur 1,00

Une analyse qui examine tous les scénarios par lequel il serait possible de pirater un système informatique particulier constitue une analyse de risque complète pour ce système

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

Question **15**

Incorrect

Note de 0,00 sur 1,00

L'analyse de risque basée sur les scénarios mets l'emphase sur les méthodes et outils technologiques dans une attaque, ainsi que sur les vulnérabilités qui pourraient être exploitées pour qu'un acteur quelconque arrive à ses fins.

Veuillez choisir une réponse.

- Vrai
- Faux ✖

La réponse correcte est « Vrai ».

Question **16**

Incorrect

Note de 0,00 sur 1,00

Nous avons mentionné 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 :

Veuillez choisir une réponse.

a. Les acteurs de menaces développent leur capacité avec le temps, que ce soit en termes de connaissance, de méthodes ou d'outils. ✖

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. L'évolution des priorités et le modèle d'affaires de la compagnie peuvent changer la probabilité et l'impact des différentes menaces.

Votre réponse est incorrecte.

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.

Question **17**

Incorrect

Note de 0,00 sur 1,00

Après avoir fait votre analyse de risque telle que vue en classe, vous évaluez que la menace A démontre un risque de 2.1, tandis que le scénario B a un risque calculé de 4.2. Que pouvez-vous conclure sur le risque des scénarios A et B ? Choisissez la meilleure réponse.

Veuillez choisir une réponse.

a. La menace A présente plus de risque que la menace B.

b. Il est absolument nécessaire de déployer une contre-mesure pour réduire le risque relié à la menace B. ✖

c. Il est fort probable que de transférer le risque, par exemple à travers une police d'assurance, soit plus couteux pour la menace B que pour la menace A.

d. Si la menace B se réalise, il faudra prévoir un budget deux fois plus pour faire face à ses conséquences que si la menace A se réalise.

Votre réponse est incorrecte.

La réponse correcte est : Il est fort probable que de transférer le risque, par exemple à travers une police d'assurance, soit plus couteux pour la menace B que pour la menace A.

◀ Support-Séance2-Exercices avec corrigé

Aller à...

Exercice Cours Analyse de Risque ▶

Commencé le	jeudi 19 janvier 2023, 13:58
État	Terminé
Terminé le	mardi 28 février 2023, 18:21
Temps mis	40 jours 4 heures
Points	11,00/18,00
Note	**6,11** sur 10,00 (**61,11**%)

Question **1**

Correct

Note de 1,00 sur 1,00

Si on garde la méthode d'encodage secrète, il n'est pas nécessaire d'utiliser un chiffrement pour garantir la confidentialité

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **2**

Incorrect

Note de 0,00 sur 1,00

Lequel de ces composants ne fait pas partie du modèle de Shannon révisé :

Veuillez choisir une réponse.

- a. Codage
- b. Chiffrement ✖
- c. Compression
- d. Canal

Votre réponse est incorrecte.

La réponse correcte est : Compression

Question **3**

Correct

Note de 1,00 sur 1,00

Dans le modèle de Shannon, à laquelle de ces informations Ève n'a pas accès :

Veuillez choisir une réponse.

- a. L'algorithme de chiffrement
- b. Les paramètres de l'algorithme de codage
- c. Le message transmis sur le canal

d. La clé de chiffrement ✔

Votre réponse est correcte.

La réponse correcte est : La clé de chiffrement

Question **4**

Correct

Note de 1,00 sur 1,00

Un codage et un chiffrement sont tous deux des formes de translitérations

Veuillez choisir une réponse.

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question **5**

Correct

Note de 1,00 sur 1,00

Il n'est pas mathématiquement correct de parler de l'entropie d'un texte. Il faut dans ce cas plutôt parler de « pseudo-entropie ».

Veuillez choisir une réponse.

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question **6**

Correct

Note de 1,00 sur 1,00

L'entropie d'une source qui émet chaque fois un symbole de l'alphabet grec (24 lettres) choisi au hasard est la même que celle qui émet chaque fois la prochaine lettre du texte de « Antigone », la fameuse pièce de théâtre du dramaturge grec du 5^{e} siècle av. J.-C., Sophocle

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **7**

Correct

Note de 1,00 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 9 ans.

Veuillez choisir une réponse.

- a. Il n'est pas nécessaire d'augmenter la taille de la clé

b. 1 bit

c. 6 bits ✔

d. 128 bits

Votre réponse est correcte.

La réponse correcte est : 6 bits

Question **8**

Incorrect

Note de 0,00 sur 1,00

Laquelle de ces sources génère le plus d'information ?

Veuillez choisir une réponse.

a. Une source qui génère pile avec une probabilité de 10% et face avec une probabilité de 90%. ✖

b. Une source qui génère pile avec une probabilité de 30% et face avec une probabilité de 70%.

c. Une source qui génère pile avec une probabilité de 60% et face avec une probabilité de 40%.

d. Une source qui génère pile avec une probabilité de 50% et face avec une probabilité de 50%.

e. Une source qui génère pile avec une probabilité de 80% et face avec une probabilité de 20%.

Votre réponse est incorrecte.

La réponse correcte est : Une source qui génère pile avec une probabilité de 50% et face avec une probabilité de 50%.

Question **9**

Correct

Note de 1,00 sur 1,00

Une source déterministe produisant 50% de 0 et 50% de 1 possède une entropie plus grande qu'une source markovienne produisant 75% de 0 et 25 % de 1.

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

Question **10**

Incorrect

Note de 0,00 sur 1,00

Laquelle de ces sources génère le plus d'information ?

Veuillez choisir une réponse.

a. Une source qui génère pile ou face en lançant une pièce de monnaie

b. Une source qui génère un chiffre de 1 à 6 en lançant un dé

c. Une source qui génère un chiffre de 1 à 6 de manière séquentielle (e.g. {1}, suivi de {2}, suivi de {3}, etc)

d. Une source qui génère pile ou face en alternance

e. Une source qui génère une chaîne de 10 caractères ASCII basée sur la vitesse de la lumière dans le vide ✖

Votre réponse est incorrecte.

La réponse correcte est : Une source qui génère un chiffre de 1 à 6 en lançant un dé

Question **11**

Incorrect

Note de 0,00 sur 1,00

Laquelle de ces sources génère le plus d'information ?

Veuillez choisir une réponse.

a. Une source markovienne déterministe

b. Une source markovienne aléatoire

c. Une source non-markovienne déterministe

d. Une source non-markovienne aléatoire ✖

e. Toutes ces sources génèrent la même quantité d'information

Votre réponse est incorrecte.

La réponse correcte est : Une source markovienne aléatoire

Question **12**

Correct

Note de 1,00 sur 1,00

Je suis entré en possession de dizaines de millions de pages de texte en anglais encodés en ASCII. Je calcule la pseudo-entropie moyenne par caractère de mon échantillon. Laquelle de ces valeurs est-ce que je devrais me rapprocher ?

Veuillez choisir une réponse.

a. Le taux de compression caractère par caractère ✔

b. 8 bits

c. 1 bit

d. L'entropie du langage

Votre réponse est correcte.

La réponse correcte est : Le taux de compression caractère par caractère

Question **13**

Incorrect

Note de 0,00 sur 1,00

Pour une source donnée, lequel de ces codages présente le taux de compression non destructeur le plus élevé ?

Veuillez choisir une réponse.

a. Un encodage binaire sur un nombre de bits égal à l'entropie

b. Un encodage binaire sur un nombre de bits égal à la moitié de l'entropie

c. Un encodage ASCII avec un nombre de bytes egal a l'entropie ✖

d. Un encodage ASCII avec un nombre de bytes égal à la moitié de l'entropie

e. Un encodage MP3

Votre réponse est incorrecte.

La réponse correcte est : Un encodage binaire sur un nombre de bits égal à l'entropie

Question **14**

Correct

Note de 1,00 sur 1,00

Il est plus facile de faire de la cryptanalyse si le message à chiffrer est de l'anglais plutôt que les résultats des derniers tirages de la Loto 6/49.

Veuillez choisir une réponse.

Vrai ✔

Faux

La réponse correcte est « Vrai ».

Question **15**

Correct

Note de 1,00 sur 1,00

L'entropie d'une source est maximale pour une source sans mémoire dont tous les symboles se retrouvent dans la même proportion dans un texte statistiquement représentatif de la source.

Veuillez choisir une réponse.

Vrai ✔

Faux

La réponse correcte est « Vrai ».

Question **16**

Incorrect

Note de 0,00 sur 1,00

Choisissez la réponse la plus appropriée pour cette affirmation « Si l'algorithme de chiffrement est vulnérable, il est très facile de faire la cryptanalyse fréquentielle d'une source markovienne dont tous les caractères sont équiprobables ».

Veuillez choisir une réponse.

a. Vrai, si l'algorithme est vulnérable, l'analyse fréquentielle n'est plus nécessaire

b. Faux, la distribution statistique du texte chiffré ne présentera pas de variation significative de fréquences

c. Vrai, il suffit de comparer les fréquences des caractères avec la fréquence des lettres en langue anglaise

d. Faux, dès que le texte est chiffré, il est impossible de faire de l'analyse fréquentielle.

e. Vrai, uniquement l'analyse des digrammes et des trigrammes sera affectée par les caractéristiques de la source ✖

Votre réponse est incorrecte.

La réponse correcte est : Vrai, si l'algorithme est vulnérable, l'analyse fréquentielle n'est plus nécessaire

Question **17**

Incorrect

Note de 0,00 sur 1,00

Le principe qui dit que la sécurité d'un algorithme de cryptographie ne devrait dépendre que du secret de la clé

Veuillez choisir une réponse.

a. s'appelle le principe de Kerchoff

b. n'est pas un principe de sécurité informatique

c. a été énoncé par les inventeurs de l'algorithme RSA (Rivest, Shamir, Adleman)

d. ne s'applique qu'aux algorithmes de cryptographie à clé secrète ✖

Votre réponse est incorrecte.

La réponse correcte est : s'appelle le principe de Kerchoff

Question **18**

Correct

Note de 1,00 sur 1,00

L'entropie peut être une mesure décrivant la difficulté de mener les attaques suivantes, à **l'exception** de :

Veuillez choisir une réponse.

a. Une attaque de crackage de mot de passe par force brute.

b. Une attaque de déni de service par SYN flooding. ✔

c. Une attaque de « session hijacking » dans une application Web utilisant des jetons de session (session ID).

d. Une attaque de cryptanalyse par analyse fréquentielle.

Votre réponse est correcte.

La réponse correcte est : Une attaque de déni de service par SYN flooding.

◀ Support-Séance3-Exercices Aller à... Exercice Cours Crypto 1 ▶

Commencé le	jeudi 19 janvier 2023, 13:58
État	Terminé
Terminé le	jeudi 2 mars 2023, 00:23
Temps mis	41 jours 10 heures
Points	6,00/15,00
Note	**4,00** sur 10,00 (**40**%)

Question **1**

Incorrect

Note de 0,00 sur 1,00

En considérant un chiffrement 3DES en mode chiffrement par bloc (Electronic Code Book), lequel de ces encodages limite au maximum les chances de l'attaquant ?

Veuillez choisir une réponse.

a. Un encodage binaire sur un nombre de bits égal à l'entropie avec bourrage de zéros

b. Un bourrage de zéros suivi d'un encodage ASCII ✖

c. Un encodage binaire sur un nombre de bits égal à l'entropie avec bourrage aléatoire

d. Un encodage ASCII avec bourrage aléatoire

e. Un encodage binaire sur un nombre de bits égal à l'entropie avec bourrage de uns

Votre réponse est incorrecte.

La réponse correcte est : Un encodage binaire sur un nombre de bits égal à l'entropie avec bourrage aléatoire

Question **2**

Correct

Note de 1,00 sur 1,00

Vous disposez d'une source parfaitement aléatoire qui produit des messages de 64 bits. Vous êtes contraint à faire passer vos messages dans un canal chiffré par 3DES utilisé en mode bloc (Electronic Code Book). Comment vous assurer que l'utilisation du mode bloc ne compromet pas la sécurité de vos données ?

Veuillez choisir une réponse.

a. Compresser la source

b. Utiliser du bourrage aléatoire

c. Faire un XOR du message chiffré avec un vecteur d'initialisation.

d. Chiffrer une seconde fois

e. Aucune de ces techniques n'est nécessaire tant que l'attaquant ne peut pas faire d'attaque à texte connu ✔

Votre réponse est correcte.

La réponse correcte est : Aucune de ces techniques n'est nécessaire tant que l'attaquant ne peut pas faire d'attaque à texte connu

Question **3**

Correct

Note de 1,00 sur 1,00

Quel est l'objectif principal de l'utilisation d'algorithme de chiffrement par bloc, tel que DES, en mode de chaînage de bloc (Cipher Bloc Chaining) ?

Veuillez choisir une réponse.

a. Éviter que deux blocs chiffrés se déchiffrent avec la même clé

b. Améliorer la vitesse de déchiffrement

c. Tromper les attaquants sur le mode de chiffrement

d. Prévenir que deux messages identiques donnent le même bloc chiffré ✔

e. Ajouter le nombre de bit du vecteur d'initialisation à la taille effective de la clé

Votre réponse est correcte.

La réponse correcte est : Prévenir que deux messages identiques donnent le même bloc chiffré

Question **4**

Incorrect

Note de 0,00 sur 1,00

Vous êtes en possession d'une boîte noire qui fait 1 000 000 de déchiffrements à la seconde. Quel est le temps nécessaire pour monter une attaque par force brute à l'aide d'un texte connu (vous possédez un exemplaire chiffré et déchiffré du même texte) pour un algorithme ayant une taille effective de clé de 56 bits ?

Veuillez choisir une réponse.

a. Approximativement 14 millions d'années ✖

b. Approximativement 1 000 ans

c. Approximativement 2 000 ans

d. Approximativement 5 700 ans

e. Approximativement 11 400 ans

Votre réponse est incorrecte.

La réponse correcte est : Approximativement 2 000 ans

Question **5**

Correct

Note de 1,00 sur 1,00

Il est "raisonnablement" possible de réaliser une attaque de force brute sur un algorithme de substitution mono alphabétique si l'alphabet de source ne contient que 28 lettres.

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

Question **6**

Correct

Note de 1,00 sur 1,00

Parmi les tailles de clés suivantes, laquelle est la plus appropriée pour un chiffrement AES ?

Veuillez choisir une réponse.

a. 56 bits.

b. 64 bits.

c. 128 bits. ✔

d. 2048 bits.

Votre réponse est correcte.

La réponse correcte est : 128 bits.

Question **7**

Correct

Note de 1,00 sur 1,00

Il n'est pas possible de réaliser une attaque de force brute par essai de toutes les clés pour l'algorithme AES avec une quantité de ressources raisonnable.

Veuillez choisir une réponse.

Vrai ✔

Faux

La réponse correcte est « Vrai ».

Question **8**

Incorrect

Note de 0,00 sur 1,00

L'utilisation de l'algorithme de chiffrement 3DES est préférable à celle de l'algorithme AES car elle assure un niveau de protection adéquat et une meilleure performance

Veuillez choisir une réponse.

Vrai ✖

Faux

La réponse correcte est « Faux ».

Question **9**

Correct

Note de 1,00 sur 1,00

Étant donné que le vecteur d'initialisation (IV) utilisé dans les algorithmes de chiffrement par flux est rendu public par Alice lorsqu'elle l'envoie à Bob, n'importe quelles valeurs peuvent être choisies par Alice pour l'IV lors de ses transmissions à Bob.

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

Question **10**

Incorrect

Note de 0,00 sur 1,00

Il n'est pas possible d'utiliser un algorithme à clé symétrique pour faire des signatures numériques.

Veuillez choisir une réponse.

- Vrai ✖
- Faux

La réponse correcte est « Faux ».

Question **11**

Incorrect

Note de 0,00 sur 1,00

L'utilisation de la cryptanalyse fréquentielle permet d'avoir des gains considérables par rapport à l'utilisation de la force brute contre la méthode de chiffrement AES, même si l'entropie de la source est élevée.

Veuillez choisir une réponse.

- Vrai ✖
- Faux

La réponse correcte est « Faux ».

Question **12**

Incorrect

Note de 0,00 sur 1,00

L'analyse fréquentielle est la meilleure méthode de cryptanalyse contre l'algorithme de chiffrement à masque jetable (connu aussi comme « one-time pad » ou algorithme de Vernam).

Veuillez choisir une réponse.

- Vrai ✖
- Faux

La réponse correcte est « Faux ».

Question **13**

Incorrect

Note de 0,00 sur 1,00

L'algorithme du masque jetable est un algorithme de chiffrement dit « parfait », car la confidentialité du message est toujours assurée, quelle que soit l'entropie de la source générant le message, à condition que la clé soit aussi longue que le message et que celle-ci soit générée avec un maximum d'entropie.

Veuillez choisir une réponse.

- Vrai
- Faux ✖

La réponse correcte est « Vrai ».

Question **14**

Incorrect

Note de 0,00 sur 1,00

L'algorithme du masque jetable est le seul algorithme dit « parfait » pour toutes ces raisons à l'exception de :

Veuillez choisir une réponse.

a. Sa sécurité est basée sur l'impossibilité mathématique de factoriser de grands chiffres entiers en temps polynomial.

b. Quelle que soit l'entropie de la source, le message ne peut pas être déchiffré par force brute ni par analyse fréquentielle, en supposant que la clé à une entropie maximale est aussi longue que le message ✖

c. Les opérations arithmétiques nécessaires peuvent être facilement implémentés en matériel, sur un microprocesseur et même facilement calculé par un humain.

d. Il suit le principe de « Kerckhoffs ».

Votre réponse est incorrecte.

La réponse correcte est : Sa sécurité est basée sur l'impossibilité mathématique de factoriser de grands chiffres entiers en temps polynomial.

Question **15**

Incorrect

Note de 0,00 sur 1,00

Lors de l'utilisation de la technique du masque jetable (one-time pad) aussi connu sous le nom d'algorithme de Vernam, pour un texte de 2000 caractères ASCII, quelle sera la longueur de la clé ?

Veuillez choisir une réponse.

a. 64 bits

b. 128 bits

c. 2024 bits ✖

d. 16000 bits

e. 64000 bits

Votre réponse est incorrecte.

La réponse correcte est : 16000 bits

◀ Support-Séance4-Cours Aller à... Support-Séance-Exercices ▶

Commencé le	vendredi 3 mars 2023, 22:55
État	Terminé
Terminé le	vendredi 3 mars 2023, 23:09
Temps mis	14 min 21 s
Points	10,00/14,00
Note	**7,14** sur 10,00 (**71,43**%)

Question **1**

Incorrect

Note de 0,00 sur 1,00

Vous désirez mettre en place une politique de vérification de mots de passe pour vous assurer que les mots de passes choisis par vos usagers ne soient pas trop faibles, tout en étant facile à retenir par vos usagers. Deux politiques vous sont proposées : 1) choisir des mots de passe composés de 6 caractères (lettres minuscules a-z, majuscules A-Z et chiffres 0-9) choisis au hasard et 2) choisir une « phrase » de passe composé de quatre mots du français courant, choisis au hasard dans un dictionnaire de 1 000 mots. D'un point de vue de sécurité, la première option est plus désirable.

Veuillez choisir une réponse.

- Vrai ✖
- Faux

La réponse correcte est « Faux ».

Question **2**

Correct

Note de 1,00 sur 1,00

Laquelle de ces solutions d'authentification constitue une solution d'authentification à « deux facteurs » ?

Veuillez choisir une réponse.

- a. Après la saisie de code d'usager et mot de passe, l'envoi d'un code par SMS sur votre téléphone cellulaire que vous devez taper ensuite sur la page d'authentification ✔
- b. Après la saisie de code d'usager et mot de passe, avoir à répondre à une question de sécurité dont la réponse est secrète
- c. Insérer une carte à puces dans le lecteur de carte à puces connecté à un ordinateur pour s'y identifier
- d. Une application nécessitant que deux usagers s'authentifient avec leurs mots de passe respectifs afin de réaliser une transaction sensible et importante

Votre réponse est correcte.

La réponse correcte est : Après la saisie de code d'usager et mot de passe, l'envoi d'un code par SMS sur votre téléphone cellulaire que vous devez taper ensuite sur la page d'authentification

Question **3**

Correct

Note de 1,00 sur 1,00

Laquelle de ces réponses ne constitue pas un facteur d'authentification :

Veuillez choisir une réponse.

a. Quelque chose qu'on a

b. Quelque chose qu'on est

c. Quelque chose qu'on imite ✔

d. Quelque chose qu'on connait

Votre réponse est correcte.

La réponse correcte est : Quelque chose qu'on imite

Question **4**

Correct

Note de 1,00 sur 1,00

Lors d'une authentification mutuelle, laquelle de ces étapes n'est pas réalisée :

Veuillez choisir une réponse.

a. Le serveur s'authentifie au client

b. Le client s'authentifie au serveur

c. Le serveur fait parvenir son certificat de clé privée au client ✔

d. Le client contacte le serveur pour initier la connexion

Votre réponse est correcte.

La réponse correcte est : Le serveur fait parvenir son certificat de clé privée au client

Question **5**

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

Veuillez choisir une réponse.

a. Le serveur envoie un code de 4 chiffres par SMS au numéro de téléphone cellulaire de l'usager enregistré pour l'usager concerné

b. 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

c. L'usager doit taper le contenu d'un captcha qui apparait sur la page Web d'authentification et change à chaque fois ✔

d. 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

Votre réponse est correcte.

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

Question **6**

Incorrect

Note de 0,00 sur 1,00

Laquelle de ces exemples de systèmes d'authentification ne constitue pas un système d'authentification à deux facteurs

Veuillez choisir une réponse.

a. Un guichet de contrôle d'accès physique exige que l'usager dépose la paume de sa main après avoir rentré un code secret à 9 chiffres qui est unique à cet usager.

b. Pour gagner accès à une zone d'accès restreint, un employé doit dire une phrase secrète concrète qu'un système de traitement de la voix reconnait comme étant la bonne phrase. De plus le système est capable de reconnaître que c'est bien lui qui a prononcé la phrase.

c. Un site bancaire demande à un usager de répondre à une « question de sécurité » supplémentaire après que l'usager ait rentré son numéro de carte bancaire et son Numéro d'identification personnel (NIP).

d. Un chien de garde très méchant reconnait les membres de son foyer par leur odeur et monte la garde devant la porte de la maison qui est barrée à clé. ✖

Votre réponse est incorrecte.

La réponse correcte est : Un site bancaire demande à un usager de répondre à une « question de sécurité » supplémentaire après que l'usager ait rentré son numéro de carte bancaire et son Numéro d'identification personnel (NIP).

Question **7**

Correct

Note de 1,00 sur 1,00

Votre ancienne politique de mots de passe forçait vos usagers à utiliser un mot de passe d'exactement 6 caractères alphabétique en minuscules (a-z). Pour renforcer la sécurité, vous demandez maintenant des mots de passe de 8 caractères, pouvant contenir des minuscules, majuscules et chiffres (a-z + A-Z + 0-9). De combien de bits effectifs avez-vous renforcé le mot de passe si on considère que vos usagers choisissent des mots de passe complètement aléatoires ?

Veuillez choisir une réponse.

a. Augmentation de 1.3 bits effectifs.

b. Augmentation de 19.4 bits effectifs. ✔

c. Diminution de 2 bits effectifs.

d. Augmentation de 5.8 bits effectifs.

e. Augmentation de 32 bits effectifs.

Votre réponse est correcte.

La réponse correcte est : Augmentation de 19.4 bits effectifs.

Question **8**

Incorrect

Note de 0,00 sur 1,00

Laquelle de ces méthodes de contrôle d'accès représente un contrôle d'authentification à deux facteurs

Veuillez choisir une réponse.

a. Scan de l'iris et lecture d'empreintes digitales ✖

b. Jeton d'authentification (e.g. jeton SecurID)

c. Mot de passe et question secrète

d. Poignée de main secrète et bague symbole des Francs-Maçons

Votre réponse est incorrecte.

La réponse correcte est : Poignée de main secrète et bague symbole des Francs-Maçons

Question **9**

Correct

Note de 1,00 sur 1,00

Laquelle de ces affirmations illustre un des principaux désavantages de la biométrie ?

Veuillez choisir une réponse.

a. Haut taux de faux positifs.

b. La base de données de données biométriques est beaucoup plus grande que le stockage de hachés de mots de passe

c. Plus facile à cracker qu'un mot de passe puisque l'entropie est faible

d. La technologie de lecture d'empreintes digitales n'est pas au point

e. Lorsque les données biométriques sont compromises, il est difficile pour l'utilisateur de les changer ✔

Votre réponse est correcte.

La réponse correcte est : Lorsque les données biométriques sont compromises, il est difficile pour l'utilisateur de les changer

Question **10**

Incorrect

Note de 0,00 sur 1,00

Si l'on utilise une technique d'authentification par preuve à connaissance nulle, le serveur doit connaître le secret qui permet au client de s'authentifier

Veuillez choisir une réponse.

Vrai ✖

Faux

La réponse correcte est « Faux ».

Question **11**

Correct

Note de 1,00 sur 1,00

Où peut-on trouver les informations sur les mots de passe des usagers dans la plupart des distributions Linux modernes ?

Veuillez choisir une réponse.

a. La mémoire vive

b. Le fichier /etc/passwd

c. Le fichier /etc/shadow ✔

d. Le fichier /dev/null

e. La commande passwd

Votre réponse est correcte.

La réponse correcte est : Le fichier /etc/shadow

Question **12**

Correct

Note de 1,00 sur 1,00

Sur les plus récentes plateformes Linux, l'accès au fichier /etc/shadow est protégé en lecture puisqu'il contient les mots de passe des usagers en clair.

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

Question **13**

Correct

Note de 1,00 sur 1,00

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.

Veuillez choisir une réponse.

Vrai ✔

Faux

La réponse correcte est « Vrai ».

Question **14**

Correct

Note de 1,00 sur 1,00

L'utilisation d'une méthode d'authentification par « défi-réponse » permet de se protéger contre l'interception de la session d'authentification

Veuillez choisir une réponse.

Vrai ✔

Faux

La réponse correcte est « Vrai ».

◀ Support-Séance5-Cours Aller à... Support-Séance5-Exercices ▶

Commencé le	samedi 4 mars 2023, 19:38
État	Terminé
Terminé le	dimanche 5 mars 2023, 01:30
Temps mis	5 heures 52 min
Points	14,00/23,00
Note	**6,09** sur 10,00 (**60,87**%)

Question **1**

Correct

Note de 1,00 sur 1,00

Si Alice veut envoyer un message confidentiel à Bob en utilisant le chiffrement RSA, quelle opération doit-elle faire?

Veuillez choisir une réponse.

a. Chiffrer avec la clé privée d'Alice

b. Chiffrer avec la clé privée de Bob

c. Chiffrer avec la clé publique d'Alice

d. Chiffrer avec la clé publique de Bob ✔

e. Chiffrer avec un secret partagé

Votre réponse est correcte.

La réponse correcte est : Chiffrer avec la clé publique de Bob

Question **2**

Incorrect

Note de 0,00 sur 1,00

Si Alice veut prouver à tout le monde qu'un document a vraiment été produit par elle, quelle opération doit-elle faire ?

Veuillez choisir une réponse.

a. Chiffrer avec sa clé publique ✖

b. Chiffrer avec un secret partagé

c. Chiffrer avec sa clé privée

d. Utiliser une fonction de hachage cryptographique

e. Utiliser un certificat

Votre réponse est incorrecte.

La réponse correcte est : Chiffrer avec sa clé privée

Question **3**

Correct

Note de 1,00 sur 1,00

Les chiffrements probabilistes tels qu'El-Gamal ou le chiffrement à courbes elliptiques sont très vulnérables aux attaques par dictionnaire

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **4**

Incorrect

Note de 0,00 sur 1,00

L'utilisation de RSA doit être privilégiée par rapport à l'utilisation d'AES puisque la longueur d'une clé RSA est plus grande que la longueur d'une clé AES.

Veuillez choisir une réponse.

- Vrai ✖
- Faux

La réponse correcte est « Faux ».

Question **5**

Correct

Note de 1,00 sur 1,00

Pour utiliser El-Gamal ou les chiffrements à courbe elliptiques, puisque la valeur aléatoire peut être n'importe quelle valeur et que vous n'avez pas à la conserver, le choix de la valeur aléatoire est peu important.

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **6**

Incorrect

Note de 0,00 sur 1,00

Si on arrivait à construire un ordinateur quantique ayant seulement quelques milliers de bits quantiques (« qubit ») de mémoire, il serait possible de réaliser une attaque par force brute sur l'algorithme AES-256 en quelques minutes.

Veuillez choisir une réponse.

- Vrai ✖
- Faux

La réponse correcte est « Faux ».

Question **7**

Si on arrivait à construire un ordinateur quantique ayant seulement quelques milliers de bits quantiques

Correct

Note de 1,00 sur 1,00

(« qubit ») de mémoire, il serait possible de réaliser en quelques secondes une attaque par factorisation sur tous les algorithmes de clé publique utilisés présentement.

Veuillez choisir une réponse.

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question **8**

Correct

Note de 1,00 sur 1,00

L'algorithme cryptographique à clé publique de El-Gamal peut être défini sur n'importe quel groupe, même s'il n'est pas commutatif.

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **9**

Incorrect

Note de 0,00 sur 1,00

L'ajout de 3 bits de clé double l'effort de cryptanalyse sur l'algorithme RSA par les meilleures méthodes connues pour ce faire.

Veuillez choisir une réponse.

- Vrai
- Faux ✖

La réponse correcte est « Vrai ».

Question **10**

Correct

Note de 1,00 sur 1,00

La découverte d'un algorithme permettant de générer efficacement et rapidement des collisions dans les fonctions de hachage cryptographique commune telles que MD5 et SHA-1 permettrait à un pirate informatique de pouvoir intercepter toutes les communications entre n'importe quel site bancaire et les clients qui s'y connecte.

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **11**

Correct

La raison principale pour laquelle il est utile d'utiliser des algorithmes de cryptographie à courbes elliptiques est parce qu'il est possible d'obtenir un niveau de sécurité équivalent en utilisant des clés cryptographiques

Note de 1,00 sur 1,00

est parce qu'il est possible d'obtenir un niveau de sécurité équivalent en utilisant des clés cryptographiques plus petites, ce qui a des avantages en termes de performance.

Veuillez choisir une réponse.

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question **12**

Correct

Note de 1,00 sur 1,00

Les algorithmes de stéganographie qui permettent de cacher des messages textes dans des images constituent un outil de sécurité informatique permettant d'atteindre des objectifs de confidentialité

Veuillez choisir une réponse.

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question **13**

Correct

Note de 1,00 sur 1,00

Laquelle de ces notions n'est pas une propriété de la signature numérique :

Veuillez choisir une réponse.

a. Authenticité

b. Confidentialité ✔

c. Intégrité

d. Non répudiabilité

Votre réponse est correcte.

La réponse correcte est : Confidentialité

Question **14**

Incorrect

Note de 0,00 sur 1,00

Parmi les raisons évoquées ci-dessous, quelle est la raison principale pour laquelle il est utile d'inclure un préambule dans un texte que nous allons signer numériquement ?

Veuillez choisir une réponse.

a. S'assurer que le contexte du document soit bien compris par la personne qui va le lire

b. Rendre plus difficile pour Ève de trouver un texte équivalent avec la même signature

c. Permettre au vérificateur de s'assurer avec un degré raisonnable de confiance que le texte devant lui est bien celui qui a été signé, parmi l'ensemble infini de texte qui pourrait avoir la même signature ✖

d. Il n'est pas nécessaire, ni recommandé d'inclure un préambule

Votre réponse est incorrecte.

La réponse correcte est : Rendre plus difficile pour Ève de trouver un texte équivalent avec la même signature

Question **15**

Incorrect

Note de 0,00 sur 1,00

L'utilisation adéquate de bonnes fonctions de hachage cryptographique peut constituer une mesure efficace :

Veuillez choisir une réponse.

a. Pour réduire l'efficacité d'attaques visant à atteindre l'intégrité de biens informatiques

b. Pour obtenir un niveau de sécurité équivalent contre des efforts de cryptanalyse, tout en utilisant des tailles de clés et de bloc de chiffrement plus petits ✖

c. Construire des structures de données efficaces, où le temps de recherche est considérablement réduit

d. N'est plus du tout recommandé dans un contexte de sécurité informatique, étant donné les découvertes scientifiques récentes concernant les possibilités de découverte de collision dans MD5 et SHA-1

Votre réponse est incorrecte.

La réponse correcte est : Pour réduire l'efficacité d'attaques visant à atteindre l'intégrité de biens informatiques

Question **16**

Correct

Note de 1,00 sur 1,00

Plusieurs protocoles utilisent un chiffrement asymétrique pour chiffrer une clé de chiffrement symétrique. La clé symétrique est ensuite utilisée pour le reste de la communication. Pourquoi introduire cette complexité ?

Veuillez choisir une réponse.

a. Ça permet de contrer l'attaque de force brute

b. On combine la rapidité de la cryptographie asymétrique avec la robustesse de la cryptographie symétrique

c. On combine l'avantage de performance de la cryptographie symétrique avec l'avantage au niveau de la distribution de clé de la cryptographie asymétrique ✔

d. On double la longueur effective de la clé de chiffrement

Votre réponse est correcte.

La réponse correcte est : On combine l'avantage de performance de la cryptographie symétrique avec l'avantage au niveau de la distribution de clé de la cryptographie asymétrique

Question **17**

Correct

Note de 1,00 sur 1,00

Dans le cas d'une source avec une bonne entropie, quelle est la méthode la plus efficace pour attaquer RSA ?

Veuillez choisir une réponse.

a. Factorisation ✔

b. Attaque dictionnaire

c. Attaque de force brute

d. Inversement

e. Logarithme discret

Votre réponse est correcte.

La réponse correcte est : Factorisation

Question **18**

Incorrect

Note de 0,00 sur 1,00

Parmi les tailles de clés suivantes, laquelle est la plus appropriée pour un chiffrement RSA ?

Veuillez choisir une réponse.

a. 56 bits

b. 64 bits

c. 128 bits ✖

d. 256 bits

e. 2048 bits

Votre réponse est incorrecte.

La réponse correcte est : 2048 bits

Question **19**

Incorrect

Note de 0,00 sur 1,00

L'utilisation d'une infrastructure à clé publique (PKI) est souvent considérée essentielle pour l'opération sécuritaire avec un algorithme tel que RSA. De quelle attaque souhaite-t-on se protéger en implémentant ce type d'infrastructure ?

Veuillez choisir une réponse.

a. Débordement de mémoire tampon

b. Homme au milieu (man-in-the-middle)

c. Factorisation

d. Déchiffrement ✖

e. Débordement de compte de banque

Votre réponse est incorrecte.

La réponse correcte est : Homme au milieu (man-in-the-middle)

Question **20**

Correct

Note de 1,00 sur 1,00

Considérant une fonction de hachage cryptographique résistante aux collisions, laquelle de ces affirmations est fausse ?

Veuillez choisir une réponse.

a. Il est difficile de générer un message qui possède exactement le même haché qu'un autre message

b. Il est difficile de trouver le message original à partir du haché

c. Une taille de haché de 256 bits est suffisante

d. Deux messages choisis au hasard ont 1 chance sur 128 d'être identique pour un haché de 128 bits ✔

Votre réponse est correcte.

La réponse correcte est : Deux messages choisis au hasard ont 1 chance sur 128 d'être identique pour un haché de 128 bits

Question **21**

Incorrect

Note de 0,00 sur 1,00

Quelle est la différence principale et plus significative entre un système de gestion de clés publiques décentralisé et un système de gestion de clés publiques centralisés ?

Veuillez choisir une réponse.

a. Le fait que dans les systèmes hiérarchiques il y a des « racines de confiance » qui sont des autorités de certification dont les clés publiques sont reconnues par tous

b. Le fait que dans les systèmes hiérarchiques des compagnies font de l'argent en signant des certificats de clés publiques

c. L'utilisation de cryptographie symétrique plutôt que de la cryptographie asymétrique

d. Les systèmes décentralisés utilisent des serveurs répartis un peu partout dans le monde pour stocker les certificats de clé publique de ses utilisateurs ✖

Votre réponse est incorrecte.

La réponse correcte est : Le fait que dans les systèmes hiérarchiques il y a des « racines de confiance » qui sont des autorités de certification dont les clés publiques sont reconnues par tous

Question **22**

Correct

Note de 1,00 sur 1,00

Lorsque le certificat d'une autorité racine est compromis, tous les certificats signés par cette autorité doivent être considérés compromis.

Veuillez choisir une réponse.

Vrai ✔

Faux

La réponse correcte est « Vrai ».

Question **23**

Correct

Note de 1,00 sur 1,00

Lorsque le certificat d'une autorité racine est compromis, seules les communications vers les sites Web dont les certificats signés par cette autorité pourraient être interceptées.

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

◀ Support-Séance6-Cours Aller à... Support-Séance6-Exercices ▶

Commencé le	dimanche 5 mars 2023, 22:52
État	Terminé
Terminé le	dimanche 5 mars 2023, 23:02
Temps mis	10 min 21 s
Points	11,00/17,00
Note	**6,47** sur 10,00 (**64,71**%)

Question **1**

Incorrect

Note de 0,00 sur 1,00

Sous Linux, pour définir les droits suivants sur le fichier exam :

-rw-r----- 1 david profs 7627 Oct 1 12:50 exam

David doit exécuter la commande suivante :

Veuillez choisir une réponse.

a. chmod 744 exam

b. chmod 644 exam ✖

c. chmod 640 exam

d. chmod 540 exam

Votre réponse est incorrecte.

La réponse correcte est : chmod 640 exam

Question **2**

Incorrect

Note de 0,00 sur 1,00

Sous Linux, la commande « chmod 764 exam » est équivalente à la commande « chmod u=rwx, g=rx, o=r exam » sont équivalentes.

Veuillez choisir une réponse.

Vrai ✖

Faux

La réponse correcte est « Faux ».

Question **3**

Correct

Note de 1,00 sur 1,00

La gestion en mode discrétionnaire des permissions d'accès aux systèmes d'information dans le contexte de grandes entreprises et organisations est problématique à cause de plusieurs facteurs. Lequel n'en est pas un ?

Veuillez choisir une réponse.

a. Le grand nombre d'application avec des modèles de contrôle d'accès différents et indépendants.

b. La basse entropie de la matrice des permissions d'accès. ✔

c. Le grand nombre d'objets auxquels il faut restreindre l'accès.

d. Les besoins changeants d'accès à l'information par les divers usagers des systèmes.

Votre réponse est correcte.

La réponse correcte est : La basse entropie de la matrice des permissions d'accès.

Question **4**

Incorrect

Note de 0,00 sur 1,00

Dans le système de contrôle d'accès discrétionnaire implanté sous Linux :

Veuillez choisir une réponse.

a. Les permissions d'accès données à un objet doivent rester cachées et à l'abri de regard « indiscrets » de potentiels attaquants

b. Seul l'administrateur peut changer qui est le propriétaire d'un objet (« owner »), c'est-à-dire l'usager à qui « appartient » un objet dans le système informatique.

c. Seul le propriétaire d'un objet peut changer les droits d'accès sur cet objet.

d. Il n'est pas possible de changer les permissions d'un objet sans avoir un compte administrateur ✖

Votre réponse est incorrecte.

La réponse correcte est : Seul l'administrateur peut changer qui est le propriétaire d'un objet (« owner »), c'est-à-dire l'usager à qui « appartient » un objet dans le système informatique.

Question **5**

Correct

Note de 1,00 sur 1,00

Le but principal du modèle de Bell et LaPadula est de :

Veuillez choisir une réponse.

a. Empêcher les fuites illégales d'information (attaque contre la confidentialité) ✔

b. Empêcher les modifications illégales d'information (attaque contre l'intégrité)

c. Simplifier l'administration du modèle DAC

d. Empêcher un utilisateur habilité confidentiel de modifier des informations publiques

Votre réponse est correcte.

La réponse correcte est : Empêcher les fuites illégales d'information (attaque contre la confidentialité)

Question **6**

Incorrect

Note de 0,00 sur 1,00

Le but principal du modèle de RBAC est de :

Veuillez choisir une réponse.

a. Empêcher les fuites illégales d'information (attaque contre la confidentialité)

b. Empêcher les modifications illégales d'information (attaque contre l'intégrité) ✖

c. Simplifier l'administration du modèle DAC

d. Empêcher un utilisateur habilité confidentiel de modifier des informations publiques

Votre réponse est incorrecte.

La réponse correcte est : Simplifier l'administration du modèle DAC

Question **7**

Correct

Note de 1,00 sur 1,00

Dans le modèle RBAC, un utilisateur peut être affecté à plusieurs rôles :

Veuillez choisir une réponse.

Vrai ✔

Faux

La réponse correcte est « Vrai ».

Question **8**

Correct

Note de 1,00 sur 1,00

Dans le modèle RBAC, plusieurs utilisateurs peuvent être associés à une même session :

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

Question **9**

Correct

Note de 1,00 sur 1,00

Dans le modèle RBAC, si le rôle A est hiérarchiquement supérieur au rôle B, alors un utilisateur affecté au rôle B héritera des permissions du rôle A :

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

Question **10**

Correct

Note de 1,00 sur 1,00

Dans le modèle RBAC, l'héritage multiple est possible, c'est-à-dire un rôle peut hériter de plusieurs rôles :

Veuillez choisir une réponse.

Vrai ✔

Faux

La réponse correcte est « Vrai ».

Question **11**

Correct

Note de 1,00 sur 1,00

Dans le modèle RBAC, donner un exemple de contrainte que l'on ne peut vérifier qu'au moment où un utilisateur crée une session :

Veuillez choisir une réponse.

a. Contrainte de cardinalité (par exemple, un seul utilisateur peut être affecté au rôle de directeur)

b. Séparation statique des pouvoirs (SSOD)

c. Séparation dynamique des pouvoirs (DSOD) ✔

Votre réponse est correcte.

La réponse correcte est : Séparation dynamique des pouvoirs (DSOD)

Question **12**

Correct

Note de 1,00 sur 1,00

Dans le modèle ABAC, il est possible d'exprimer des règles de contrôle d'accès que l'on ne pourrait pas exprimer avec le modèle RBAC :

Veuillez choisir une réponse.

Vrai ✔

Faux

La réponse correcte est « Vrai ».

Question **13**

Correct

Note de 1,00 sur 1,00

De quel modèle AGLP (Access - Global - Local - Permissions) est-il une extension :

Veuillez choisir une réponse.

a. DAC

b. MAC

c. RBAC ✔

d. ABAC

Votre réponse est correcte.

La réponse correcte est : RBAC

Question **14**

Incorrect

Note de 0,00 sur 1,00

Le langage XACML (eXtensible Access Control Markup Language) est une implémentation du modèle :

Veuillez choisir une réponse.

a. ABAC

a. ABAC

b. RBAC

c. MAC

d. DAC ✖

Votre réponse est incorrecte.

La réponse correcte est : ABAC

Question **15**

Correct

Note de 1,00 sur 1,00

Quel devrait être le principe de base à appliquer lorsqu'on déploie une politique de contrôle d'accès :

Veuillez choisir une réponse.

a. Demander à l'administrateur système de définir la politique de contrôle d'accès

b. Demander au développeur d'implémenter le modèle RBAC dans les applications métier

c. Séparer le déploiement de la politique de sécurité de l'implémentation des applications métier ✔

d. Faire appel à un avocat

Votre réponse est correcte.

La réponse correcte est : Séparer le déploiement de la politique de sécurité de l'implémentation des applications métier

Question **16**

Incorrect

Note de 0,00 sur 1,00

Les plateformes mobiles basées sur le système d'exploitation IoS de Apple n'implémentent pas de système de contrôle d'accès, car l'usager n'a pas accès au système de fichiers.

Veuillez choisir une réponse.

Vrai ✖

Faux

La réponse correcte est « Faux ».

Question **17**

Correct

Note de 1,00 sur 1,00

Le principe de « *physical access = game over* » fait référence au fait que si un attaquant gagne un accès physique non restreint à une machine, il peut théoriquement, et avec suffisamment de temps, pirater cette machine et y devenir root. Cependant, ce principe ne s'applique pas aux machines virtuelles hébergées chez un tiers, car même si l'hébergeur a l'accès physique au serveur où elles sont hébergées, il ne connait pas le mot de passe root sur les machines virtuelles.

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

◀ Support-Séance7-Exercices-Corrigés

Aller à...

Exercice Cours Autorisation ▶