

[Tableau de bord](#) / [Mes cours](#) / [INF4420A - Sécurité informatique](#) / [Semaine #7 - 11 mars 2021 - Contrôle Périodique](#)
/ [Examen Intra Hiver 2021](#)

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



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 $\frac{1}{2}$ et celle d'apparition du 1 est $\frac{1}{4}$ et celle du 2 est également $\frac{1}{4}$. On utilise cette source pour générer une chaîne 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 :

$$\begin{aligned} H(S) &= \frac{1}{2} * \log_2(2) + \frac{1}{4} * \log_2(4) + \frac{1}{4} * \log_2(4) \\ &= \frac{1}{2} + \frac{1}{2} + \frac{1}{2} = 1,5 \text{ bits} \end{aligned}$$

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

$$10 * 1,5 = 15 \text{ bits}$$

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'utilisateur 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'utilisateur enregistré pour l'utilisateur 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'utilisateur

Votre réponse est correcte.

La réponse correcte est :

L'utilisateur 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 $\log_{36}(36^n) = \log_{36}(10^{78})$

C'est-à-dire $n = \log_{36}(10^{78}) = 78 \log_{36}(10) = 78 * 0,642 = 50$

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 minuscule + 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 : $\log_2(28) = 4.81$ 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'utilisateur 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'utilisateur est piratée.

Expliquez votre réponse.

Malgré le fait que la base de données d'utilisateur 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 canaux 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 opèrent 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 lutte contre les incendies ne réagit pas, il pourrait en résulter une catastrophe qui se compte en vie humaine.

Commentaire :