Commencé le	jeudi 11 mars 2021, 14:31
État	Terminé
Terminé le	jeudi 11 mars 2021, 16:17
Temps mis	1 heure 45 min
Points	27,00/27,00
Note	**30,00** sur 30,00 (**100**%)

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

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

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

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. La motivation dans B est trop élevé
- b. L'opportunité de B est trop élevé
- c. Le calcul du risque ne prend pas en compte la probabilité
- d. L'impact dans B est trop élevé
- e. La capacité 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 A est deux fois plus risquée que la menace B
- b. La menace A est plus risquée que la menace B
- c. La menace B est deux fois plus risquée que la menace A
- d. La menace B est plus risquée que la menace A ✔
- e. Les risques reliés aux menaces A et B sont acceptables

Votre réponse est correcte.

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

Question **10**

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 15 ans.

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

Votre réponse est correcte.

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

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 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
- c. Votre assureur en risque informatique offre une réduction de prime d'assurance si vous choisissez d'installer C
- d. Le coût d'achat de la contre mesure A est supérieur à celui de B et de C

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

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. Sa propre clé publique
- b. La clé privée d'Alice
- 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. Un algorithme à clé publique pour lequel il est très difficile de trouver la clé privée à partir de la clé publique
- b. Une entropie élevée de la source qui génère les textes à signer ✔
- c. Une fonction de hachage pour laquelle il est difficile de trouver des collisions avec un haché donné
- 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. 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

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

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

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

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

c. 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. ✔

d. Les technologies et le mode d'utilisation des systèmes d'information changent avec le temps

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 technologie de lecture d'empreintes digitales ne peut pas être contrefaite
- 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 technique par reconnaissance l'iris peut être utilisée pour authentifier un utilisateur jusqu'à 10 mètres de distance

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. 78 caractères
- b. Environ 50 caractères ✔
- c. Environ 30 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.

10^78 possibilités

Alphabet utilisé: 26 (lettres) + 10 (chiffres) = 36 symboles

Pour chaque caractère du mot de passe, il y a 36 possibilités.

Il y a donc 36^x possibilités de mot de passe, ou x est le nombre de caractère du mot de passe.

On peut donc utiliser la relation mathématique: 36^x = 10^78, ou x est le nombre de caractère du mot de passe.

36^x = 10^78

log (36^x) = log(10^78)

x*log(36) = 78*log(10)

x = 78*log(10)/log(36) = 50.119

x = environ 50 caractères

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.

Je calcule dabord l'entropie de la phrase composé de quatre mots tirés d'un dictionnaire de 4000 mots.

Chaque mot a une probabilité d'être tirée de 1/4000. On multiplie l'entropie mot par mot par 4 pour trouver l'entropie de la phrase puisqu'il s'agit d'une source markovienne.

H(P) = 4 * 4000/4000 * log(4000)/log(2) = 47.863 bits

Ensuite, je dresse la relation mathématique du mot de passe de longueur inconnu.

Chaque symbole a une probabilité d'être tirée de 1/28 (26 lettres de l'alphabet et 2 chiffre). On multiplie l'entropie par x, puisqu'il s'agit d'une source markovienne, qui est la longueur du mot de passe qu'on cherche.

H(M) = x * 28/28 * log(28)/log(2) = 4.807*x

Enfin, je fusionne les 2 formules mathématiques pour trouver la longueur du mot de passe qui donnera une entropie équivalente.

H(M) = 4.807*x = H(P)

4.807*x = 47.863

x = 9.957

x = 10 caractères

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.

En général, les méthodes d'authentification OTP se font avec un appareil que l'utilisateur possède (téléphone, porte-clé, etc..) et donc cela fait en sorte que l'authentification se fait avec ce que l'usager possède. Cela fait en sorte qu'un attaquant doit avoir accès à l'appareil en question pour accéder au compte.Aussi, comme les mots de passe qui sont générés sont temporaires, même si la base de donnée était piratée et rendue publique, l'attaquant n'aurait pas accès à l'appareil qui fournit les OTP et donc il n'aurait aucune information sur les OTP. Si le pirate veut accéder au compte, il devra trouver une façon d'avoir accès soit à l'appareil ou encore un mot de passe qui est valide dans un certain laps de temps ce qui rajoute un niveau de difficulté. L'utilisation de l'authentification OTP en plus de l'utilisation classique d'une nom d'usager et mot de passe est d'ailleurs de plus en plus utilisé pour augmenter la sécurité des comptes en particulier dans les plateformes tels que les banques.

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. Confidentialité

b. Disponibilité ✔

c. Rapidité

d. Honnêteté

e. Motivation

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

De mon point de vue, l'aspect de disponibilité est le plus important, car il est très très important que les systèmes en particulier ceux du contrôle du réacteur soit disponible lorsque nécessaire. Les systèmes de contrôle ont un rôle très important à jouer dans le fonctionnement d'une centrale nucléaire. Dans le cas où un système de contrôle ne serait pas disponible à un moment important, cela pourrait avoir des conséquences désastreuses et possiblement produire un incident nucléaire. Aussi, il est tout de même important malgré que c'est moins critique que les technologies d'information restent disponibles pour que les employés puissent réaliser leur travail et que les communications au sein de l'organisation se fasse sans problème.

Commentaire :

◄ Video cours 5 - 25 février - Authentification

Aller à...

Examen Intra Hiver 2021 (reprise) ►