Commencé le	vendredi 29 octobre 2021, 13:45
État	Terminé
Terminé le	vendredi 29 octobre 2021, 15:45
Temps mis	1 heure 59 min
Points	20,67/30,00
Note	**6,89** sur 10,00 (**69**%)

Question **1**

Correct

Note de 1,00 sur 1,00

Mission Impossible Question MI 1

Vous avez été recruté(e) comme membre de la IMF (Impossible Missions Force).

Votre mission, si vous l'acceptez, consiste à dérober les plans ultrasecrets ayant pour code INF4420A.

Pour accéder au coffre contenant les plans, vous devrez résoudre 3 défis :

- Casser une clé de chiffrement
- Découvrir une phrase de passe
- Casser un mot de passe

Vous aurez au maximum 1 heure pour résoudre chacun des défis.

Le premier défi consiste à casser une clé DES.

Il s'agit d'une clé de chiffrement :

a. Symétrique ✔

b. Asymétrique

Votre réponse est correcte.

La réponse correcte est :
Symétrique

Question **2**

Incorrect

Note de 0,00 sur 1,00

Mission Impossible Question MI 2

Vous décidez de casser la clé DES par force brute.

Combien de test aurez-vous à réaliser pour être sûr de casser la clé :

- a. Environ 72 * 10^15 tests
- b. Environ 128 * 10^21 tests
- c. Environ 40 * 10^12 tests
- d. Environ 56 * 10^18 tests ✖

Votre réponse est incorrecte.

La réponse correcte est :
Environ 72 * 10^15 tests

Question **3**

Correct

Note de 1,00 sur 1,00

Mission Impossible Question MI 3

Pour casser cette clé DES, vous disposez d'un composant super-performant qui permet de tester 2^44 clés par seconde.

Quelle est la probabilité que vous parveniez à casser la clé DES au bout d'une heure :

- a. Environ 50%
- b. 100%
- c. Environ 35%
- d. Environ 88% ✔

Votre réponse est correcte.

La clé DES est une clé de 56 bits. Comme votre composant super-performant permet de tester 2^44 clés par seconde, le temps nécessaire pour tester toutes les combinaisons est donc égal à :

T = 2^56 / 2^44 = 2^12 secondes = 4096 secondes

Vous disposez d'une heure, soit de 3600 secondes

La probabilité de casser la clé DES est donc de 3600 / 4096 = 87,9 %

La réponse correcte est :
Environ 88%

Question **4**

Correct

Note de 1,00 sur 1,00

Mission Impossible Question MI 4

Good luck ! Vous avez réussi à casser la clé DES.

Vous vous attaquez maintenant au deuxième défi : la phrase de passe.

Votre collègue Ethan Hunt de l'IMF vous a transmis les informations suivantes : la phrase de passe est composée de 4 mots tirés aléatoirement dans un dictionnaire de 5000 mots.

Quelle est l'entropie de cette phrase de passe ?

a. Environ 25 bits

b. Environ 49 bits ✔

c. Environ 38 bits

d. Environ 60 bits

Votre réponse est correcte.

Le nombre de combinaisons possibles de la phrase de passe est égal à 5000^4.

L'entropie de la phrase de passe est donc égale à :

E = Log2 (5000^4) = 4 * Log2(5000) = 49,15

La réponse correcte est :
Environ 49 bits

Question **5**

Correct

Note de 1,00 sur 1,00

Mission Impossible Question MI 5

Votre composant super-performant est multi-usage : il permet de tester 2^44 phrases de passe par seconde.

Quelle est la probabilité que vous parveniez à découvrir la phrase de passe au bout d'une heure :

- a. Moins de 10%
- b. Environ 88%
- c. Environ 50%
- d. 100% ✔

Votre réponse est correcte.

Avec votre composant super-performant, le temps nécessaire pour tester toutes les combinaisons est égal à :

T = 2^49,15 / 2^44 = 2^5,15 secondes = 35,15 secondes

Vous disposez de 3600 secondes

Vous avez donc 100% de chance de casser la phrase de passe.

La réponse correcte est :
100%

Question **6**

Correct

Note de 1,00 sur 1,00

Mission Impossible Question MI 6

C’est votre jour de chance : vous avez aussi réussi à découvrir la phrase de passe.

Plus qu’un défi : casser le mot de passe.

Votre collègue Ethan vous a transmis les informations suivantes : « le mot de passe est composé de 10 caractères alphanumériques (caractères minuscules de a à z, caractères majuscules de A à Z, chiffres de 0 à 9) tirés aléatoirement. »

Quels est l’entropie du mot de passe :

a. Environ 25 bits

b. Environ 38 bits

c. Environ 49 bits

d. Environ 60 bits ✔

Votre réponse est correcte.

Il y a 62 symboles possibles. Chaque symbole est tiré aléatoirement avec une probabilité de 1/62.

L’entropie par caractère est donc égale :

E = Sigma(i = 1 à 62) 1/62 * Log2(62) = Log2(62) = 5,954

Comme la source est markovienne, l’entropie par du mot de passe est égale à 10 fois l’entropie par caractère, soit 59,54.

La réponse correcte est :
Environ 60 bits

Question **7**

Correct

Note de 1,00 sur 1,00

Mission Impossible Question MI 7

Votre composant super-performant fait toujours l'affaire puisqu'il permet de tester 2^44 mots de passe par seconde.

Quelle est la probabilité que vous parveniez à découvrir le mot de passe au bout d'une heure :

a. Environ 88%

b. Moins de 10% ✔

c. Environ 50%

d. 100%

Votre réponse est correcte.

Avec votre composant super-performant, le temps nécessaire pour tester toutes les combinaisons est égal à :

T = 2^59,54 / 2^44 = 2^15,54 secondes = 47 643,77 secondes.

Vous disposez de 3600 secondes.

La probabilité de casser le mot de passe est donc de 3600 / 47 643,77 = 7,556 %

La réponse correcte est :
Moins de 10%

Question **8**

Correct

Note de 1,00 sur 1,00

Mission Impossible Question MI 8

En utilisant votre composant super-performant qui permet de tester 2^44 mots de passe par seconde, quelle doit être l'entropie maximale du mot de passe pour être sûr à 100% de casser le mot de passe au bout d'une heure ?

- a. Environ 55,81 bits ✔
- b. Environ 47,65 bits
- c. Environ 51,35 bits
- d. Environ 53,47 bits

Votre réponse est correcte.

Soit n l'entropie du mot de passe.

Il faut qu'un bout d'une heure, on ait pu tester toutes les combinaisons du mot du mot de passe soit 2^n combinaisons.

En une heure, on aura testé 3600 * 2^44 combinaisons.

On a donc 2^n = 3600 * 2^44.

Donc n = Log2(3600 * 2^44) = Log2(3600) + 44 = 55,81

La réponse correcte est :
Environ 55,81 bits

Question **9**

Correct

Note de 1,00 sur 1,00

Mission Impossible Question MI 9

Vous recevez un second message d'Ethan :

« J'ai oublié de te dire, j'ai obtenu les informations suivantes sur la structure du mot de passe :

· Les 8 premiers caractères sont des caractères minuscules ou des caractères majuscules choisis aléatoirement.

· Concernant les deux derniers caractères, la probabilité que ce soit un chiffre est de 50%, la probabilité qu'il s'agisse d'un caractère minuscule est de 25% et la probabilité qu'il s'agisse d'un caractère majuscule est de 25%.

J'espère que ces informations te seront utiles. »

Quelle est l'entropie réelle du mot de passe ?

a. Environ 48,12 bits

b. Environ 58,94 bits

c. Environ 53,86 bits

d. Environ 56,62 bits ✔

Votre réponse est correcte.

Entropies de chacun des 8 premiers caractères :

Il y a 52 caractères possibles. Chaque symbole est tiré aléatoirement avec une probabilité de 1/52.

L'entropie par caractère est donc égale :

E = Sigma(i = 1 à 52) 1/52 * Log2(52) = Log2(52) = 5,700

Entropie de chacun des 2 derniers caractères :

La probabilité d'apparition d'un chiffre particulier dans l'un des deux derniers caractères est de ½ * 1/10 = 1/20

La probabilité d'apparition d'un caractère minuscule particulier dans l'un des deux derniers caractères est de 1/4 * 1/26 = 1/104

La probabilité d'apparition d'un caractère minuscule particulier dans l'un des deux derniers caractères est de 1/4 * 1/26 = 1/104

L'entropie par caractère est donc égale :

E = Sigma(i = 1 à 10) 1/20 * Log2(20) + Sigma(i = 1 à 26) 1/104 * Log2(104) + Sigma(i = 1 à 26) 1/104 * Log2(104)

Donc E = ½ Log2(20) + ½ Log2(104) = 4,32 / 2 + 6,70 / 2 = 5,51

L'entropie du mot de passe est donc égale à : 8 * 5,70 + 2 * 5,51 = 56,62 bits

La réponse correcte est :
Environ 56,62 bits

Question **10**

Terminer

Note de 0,00 sur 2,00

Mission Impossible Question MI 9b

Expliquez votre calcul de la Question MI 9

Nous appliquons la formule pour calculer lentropie de la source:

Pour les 8 caractères:

26 min + 26 maj = 52

H(S) = log2(1/ 1/(52)) = 5.7

Pour 8 caractères = 5.7 *8 = 45.6 bits

Pour les 2 caractères:

Chiffres: 1/2 * log2 (1/ (1/2)) = 0.5

Min: 1/4 * log2(1/ (1/4)) = 0.5

Maj: 1/4 * log2(1/ (1/4)) = 0.5

45.6 (8 caractères) + 10 (2 caractères)

= 56.62 bits

Entropies de chacun des 8 premiers caractères :

Il y a 52 caractères possibles. Chaque symbole est tiré aléatoirement avec une probabilité de 1/52.

L'entropie par caractère est donc égale :

E = Sigma(i = 1 à 52) 1/52 * Log2(52) = Log2(52) = 5,700

Entropie de chacun des 2 derniers caractères :

La probabilité d'apparition d'un chiffre particulier dans l'un des deux derniers caractères est de ½ * 1/10 = 1/20

La probabilité d'apparition d'un caractère minuscule particulier dans l'un des deux derniers caractères est de 1/4 * 1/26 = 1/104

La probabilité d'apparition d'un caractère minuscule particulier dans l'un des deux derniers caractères est de 1/4 * 1/26 = 1/104

L'entropie par caractère est donc égale :

E = Sigma(i = 1 à 10) 1/20 * Log2(20) + Sigma(i = 1 à 26) 1/104 * Log2(104) + Sigma(i = 1 à 26) 1/104 * Log2(104)

Donc E = ½ Log2(20) + ½ Log2(104) = 4,32 / 2 + 6,70 / 2 = 5,51

L'entropie du mot de passe est donc égale à : 8 * 5,70 + 2 * 5,51 = 56,62 bits

Commentaire :

Question **11**

Terminer

Note de 0,00 sur 2,00

Mission Impossible Question MI 10

En utilisant les informations de la Question MI 9, proposez un algorithme pour augmenter vos chances de casser le mot de passe.

Afin d'augmenter mes chances de casser le mot de passe, l'attaque dictionnaire serait efficace car on essaie chacun des mots du dictionnaire jusqu'à ce qu'on trouve une correspondance avec le mot chiffré. Nous savons que les 8 premiers caracteres peuvent former des mots.

Concernant les 8 premiers caractères, l'algorithme consiste à réaliser une attaque par force brute.

L'algorithme consiste ensuite à utiliser les probabilités différentes sur les 2 derniers caractères du mot de passe.

L'algorithme est donc structuré en trois parties :

Partie 1 : Force brute sur les 8 premiers caractères + Force brute sur le 9^{ième} caractère pour les chiffres + Force brute sur le 10^{ième} caractère pour les chiffres

Partie 2 :

· Partie 2a : Force brute sur les 8 premiers caractères + Force brute sur le 9^{ième} caractère pour les chiffres + Force brute sur le 10^{ième} caractère pour les caractères autres que les chiffres

· Partie 2b : Force brute sur les 8 premiers caractères + Force brute sur le 9^{ième} caractère pour les caractères autres que chiffres + Force brute sur le 10^{ième} caractère pour les chiffres

Partie 3 : Force brute sur les 8 premiers caractères + Force brute sur le 9^{ième} caractère pour les caractères autres que chiffres + Force brute sur le 10^{ième} caractère pour les caractères autres que chiffres

Commentaire :

Question **12**

Correct

Note de 1,00 sur 1,00

Mission Impossible Question MI 11

En utilisant l'algorithme de la question MI 10 et le composant super-performant qui permet de tester 2^44 mots de passe par seconde, quelle est la probabilité que vous parveniez à découvrir le mot de passe au bout d'une heure :

a. Environ 40%

b. Environ 60%

c. Plus de 75% ✔

d. Moins de 25%

Votre réponse est correcte.

Nombre de tests nécessaires pour la Partie 1 : 52^8 * 10 * 10

Temps nécessaire pour la Partie 1 :

T1 = 52^8 * 10 * 10 / 2^44 = 303,88 secondes

Nombre de tests nécessaires pour la Partie 2a : 52^8 *52 *10 = 52^9 *10

Temps nécessaire pour la Partie 2a :

T2a = 52^9 * 10 / 2^44 = 1580,19 secondes

Temps nécessaire pour la Partie 2b :

T2b = T2a = 1580,19 secondes

Nombre de tests nécessaires pour la Partie 3 : 52^8 *52 *52 = 52^10

Temps nécessaire pour la 3 :

T3 = 52^10 / 2^44 = 8217,01 secondes

On a T1 + T2a + T2b = 303,88 + 1580,19 + 1580,19 = 3464,26 secondes

En 1 heure, soit 3600 secondes, on peut donc réaliser les parties 1, 2a et 2b.

Et il reste 3600 – 3464,26 = 135,74 secondes

Les chances de réussite pour la partie 1 et de la partie 3 sont chacune de 0,5 * 0,5 = 25%

Les chances de réussite des partie 2a et 2b sont respectivement de 25%. Donc les chances de réussite de la partie 2 est de 50%.

Au final, la probabilité de trouver le mot de passe est donc de :

P = 25% (partie 1) + 50 (partie 2) + 135,74 / 8217,01 (partie 3) = 76,65 %

La réponse correcte est :
Plus de 75%

Question **13**

Terminer

Note de 0,00 sur 2,00

Mission Impossible Question MI 11b

Expliquez votre calcul de la Question MI 11

On a beaucoup de mots par heures et pas

Nombre de tests nécessaires pour la Partie 1 : 52^8 * 10 * 10

Temps nécessaire pour la Partie 1 :

T1 = 52^8 * 10 * 10 / 2^44 = 303,88 secondes

Nombre de tests nécessaires pour la Partie 2a : 52^8 *52 *10 = 52^9 *10

Temps nécessaire pour la Partie 2a :

T2a = 52^9 * 10 / 2^44 = 1580,19 secondes

Temps nécessaire pour la Partie 2b :

T2b = T2a = 1580,19 secondes

Nombre de tests nécessaires pour la Partie 3 : 52^8 *52 *52 = 52^10

Temps nécessaire pour la 3 :

T3 = 52^10 / 2^44 = 8217,01 secondes

On a T1 + T2a + T2b = 303,88 + 1580,19 + 1580,19 = 3464,26 secondes

En 1 heure, soit 3600 secondes, on peut donc réaliser les parties 1, 2a et 2b.

Et il reste 3600 – 3464,26 = 135,74 secondes

Les chances de réussite pour la partie 1 et de la partie 3 sont chacune de 0,5 * 0,5 = 25%

Les chances de réussite des partie 2a et 2b sont respectivement de 25%. Donc les chances de réussite de la partie 2 est de 50%.

Au final, la probabilité de trouver le mot de passe est donc de :

P = 25% (partie 1) + 50 (partie 2) + 135,74 / 8217,01 (partie 3) = 76,65 %

Commentaire :

Question **14**

Non répondue

Noté sur 1,00

Mission Impossible Question MI 12

Comparer la probabilité obtenue à la question MI 11 avec celle que l'on aurait obtenue en utilisant l'entropie calculée à la question MI 8. Expliquer pourquoi les résultats obtenus sont différents.

L'entropie réelle du mot de passe est de 56,62 bits.

Si l'on suppose que la probabilité de casser le mot de passe évolue linéairement, la probabilité de casser le mot de passe serait égale à :

P' = Max (1, 3600 / (2^56,62 / 2^44)) = 3600 / 2^12,62 = 57,19%

La probabilité P' est inférieure, car avec l'algorithme de la question MI 9, la probabilité n'évolue pas linéairement : elle évolue beaucoup plus vite au cours des parties 1 et 2 qu'avec la partie 3.

Question **15**

Correct

Note de 1,00 sur 1,00

Si Bob veut vérifier qu'un document signé électroniquement par Alice a vraiment été produit par elle, quelle opération doit-it faire ?

a. Déchiffrer avec sa clé privée

b. Déchiffrer avec la clé privée d'Alice

c. Déchiffrer avec sa clé publique

d. Déchiffrer avec la clé publique d'Alice ✔

Votre réponse est correcte.

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

Question **16**

Correct

Note de 1,00 sur 1,00

Dans l'état actuel des connaissances et tant qu'il n'existe pas d'ordinateur quantique, quelle est la complexité du meilleur algorithme pour casser une clé RSA de n bits :

a. O(n^3)

b. O(2^(n/3)) ✔

c. O(2^(n/2))

d. O(2^n)

Votre réponse est correcte.

La réponse correcte est :
O(2^(n/3))

Question **17**

Correct

Note de 1,00 sur 1,00

Dans l'état actuel des connaissances, comment faudra-t-il modifier la longueur d'une clé AES lorsqu'il existera un ordinateur quantique :

a. Il ne sera pas nécessaire de modifier la clé, l'ordinateur quantique n'aura pas d'impact sur le chiffrement symétrique

b. Il sera nécessaire de doubler la longueur de la clé ✔

c. Il ne servira à rien de modifier la longueur de la clé car l'ordinateur quantique pourra casser la clé même si sa longueur est très grande

d. Il sera nécessaire de triplet la longueur de la clé

Votre réponse est correcte.

La réponse correcte est :
Il sera nécessaire de doubler la longueur de la clé

Question **18**

Correct

Note de 1,00 sur 1,00

Un pirate montre qu'il est possible de récupérer le mot de passe d'un iPhone lors d'un partage de connexion. S'agit-il :

- a. **D'une vulnérabilité ?** ✔
- b. D'une probabilité ?
- c. D'un risque ?
- d. D'une menace ?

Votre réponse est correcte.

La réponse correcte est :
D'une vulnérabilité ?

Question **19**

Incorrect

Note de 0,00 sur 1,00

Elliot est surpris de ne plus pouvoir accéder à un fichier censé être partagé. Il mène son enquête et réussi à obtenir les informations suivantes :

- Aucun membre de son groupe (y compris lui) n'a obtenu les droits d'accès au fichier.
- En revanche d'autres utilisateurs et groupes se sont vu accorder des droits d'accès à ce fichier et au dossier contenant ce fichier
- Un gestionnaire de projet de votre équipe précise qu'il a mis à jour les permissions sur le fichier et le dossier en question dernièrement.

Selon les informations qu'Elliot a recueillies, quel type de contrôle d'accès est utilisé ici ?

- a. RBAC ✖
- b. ABAC
- c. MAC
- d. DAC

Votre réponse est incorrecte.

La réponse correcte est :
DAC

Question **20**

Correct

Note de 1,00 sur 1,00

Dans une analyse de risques, pour chaque couple menace/vulnérabilité, il faut déterminer le niveau de risque pour le système informatique, d'après les facteurs suivants :

a. La probabilité que la menace exploite la vulnérabilité

b. L'impact de l'exploitation de la vulnérabilité par la menace

c. L'adéquation des contrôles de sécurité existants visant à supprimer ou à réduire les risques

d. Tous les facteurs précités ci-dessus ✔

Votre réponse est correcte.

La réponse correcte est :
Tous les facteurs précités ci-dessus

Question **21**

Correct

Note de 1,00 sur 1,00

Vous avez mis en place une authentification à deux facteurs. Le premier facteur est une authentification par mot de passe. Le second facteur est une authentification par reconnaissance d'empreinte digitale.

Quels sont les deux facteurs présents dans cette solution d'authentification :

a. Quelque chose que je connais et quelque chose que je possède

b. Quelque chose que je possède et quelque chose que je suis

c. Quelque chose que je connais et quelque chose que je suis ✔

d. Quelque chose que je suis et quelque chose que je fais

Votre réponse est correcte.

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

Question **22**

Correct

Note de 1,00 sur 1,00

Suite de la question précédente

Vous soupçonnez des attaques réussies contre la solution d'authentification à deux facteurs que vous avez mis en place dans la question précédente.

Vous décidez de mettre en œuvre un troisième facteur d'authentification différent des deux premiers facteurs.

Quel facteur serait candidat (plusieurs réponses possibles) :

- [x] a. Envoi d'un code par SMS sur votre téléphone cellulaire que vous devez taper ensuite pour vous authentifier ✔
- [x] b. Dispositif qui vous demande de signer manuellement et qui vérifie que c'est vous qui avez signé ✔
- [ ] c. Avoir à répondre à une question de sécurité dont la réponse est secrète
- [ ] d. Dispositif de reconnaissance de votre iris

Votre réponse est correcte.

Les réponses correctes sont :
Envoi d'un code par SMS sur votre téléphone cellulaire que vous devez taper ensuite pour vous authentifier,

Dispositif qui vous demande de signer manuellement et qui vérifie que c'est vous qui avez signé

Question **23**

Partiellement correct

Note de 0,67 sur 1,00

Imaginez un système qui exécute deux types de processus différents. Au niveau de sécurité le plus bas, il exécute tous les processus qui fonctionnent sur le réseau, tandis qu'au niveau supérieur, il y a les processus de l'utilisateur qui peuvent lire des données critiques (par exemple les informations sur les cartes de crédit).

Nous voulons appliquer le modèle de Bell-LaPadula en considérant que le niveau "Réseau" est inférieur au niveau "Utilisateur".

Supposons maintenant qu'un utilisateur a accidentellement installé et lancé un cheval de Troie qui veut envoyer les données de l'utilisateur à l'auteur de ce malware. Analysez l'attaque :

- [ ] a. Le malware va pouvoir déplacer les données critiques vers un autre répertoire utilisateur
- [x] b. Le malware va pouvoir exfiltrer des données ✖
- [x] c. Le malware va pouvoir modifier des données critiques ✔
- [x] d. Le malware va pouvoir ajouter des données ✔

Votre réponse est partiellement correcte.

Vous en avez sélectionné correctement 2.
Les réponses correctes sont :
Le malware va pouvoir modifier des données critiques,

Le malware va pouvoir déplacer les données critiques vers un autre répertoire utilisateur,

Le malware va pouvoir ajouter des données

Question **24**

Terminer

Note de 2,00 sur 2,00

Citer deux cas possibles pour lesquels la connaissance de votre mot de passe par un pirate informatique n’est pas suffisante pour ouvrir une session à votre insu ?

Afin d'ouvrir une session, la connaissance du mot de passe n'est pas suffisante car le système peut détecter l'emplacement de la connexion. Ainsi, pour protéger les utilisateurs contre les pirates :

1) Le système émet un challenge avec une réponse que seul le vrai utilisateur connait l'information.

2) Le système peut utiliser l'authentification deux facteurs (par ex: envoyer un code sur le numéro de téléphone de l'usager).

Exemple 1 : Authentification 2 facteurs. Si je me fais voler mon mot de passe, il faut que casser un deuxième facteur (par exemple, empreinte digitale) pour s'authentifier.

Exemple 2 : One time password. Le mot de passe est valable une seule fois.

Exemple 3 : Authentification contextuelle. Par exemple, vérification que je suis bien chez moi ou que je me connecte d'une machine qui possède une certaine adresse IP.

Commentaire :

Question **25**

Correct

Note de 1,00 sur 1,00

Valérie a acheté un nouveau clavier sans fil qu'elle utilise avec son ordinateur personnel.

Marc, le mari de Valérie, est très jaloux. Valérie a déjà surpris Marc en train de consulter la messagerie de Valérie sur son téléphone cellulaire. Marc n'a pas de connaissance en cybersécurité.

Tom, le fils de Valérie, a 12 ans. Tom aime beaucoup sa maman mais Valérie l'a récemment puni à cause de ses mauvaises notes en classe. Il est très intéressé par la cybersécurité. Il a déjà participé à plusieurs challenges Capture the Flag.

Valérie utilise son ordinateur pour échanger avec des ami(e)s et avec les professeurs de Tom.

Quelle sont les erreurs dans l'analyse de risque suivante ?(plusieurs réponses possibles)

Scénario	Capacité	Opportunité	Motivation	Probabilité	Impact	Risque
A) Marc utilise un sniffer pour écouter les communications entre le clavier et l'ordinateur de Valérie	4	3	2	3	4	12
B) Tom utilise un sniffer pour écouter les communications entre le clavier et l'ordinateur de Valérie	2	3	4	3	4	12

- [x] a. La motivation dans B est trop haute ✔
- [x] b. La capacité dans A est trop haute ✔
- [ ] c. L'opportunité dans A est trop haute
- [ ] d. La probabilité dans B est trop basse

Votre réponse est correcte.

Les réponses correctes sont :
La capacité dans A est trop haute,

La motivation dans B est trop haute

Question **26**

Correct

Note de 1,00 sur 1,00

Suite de la question précédente

Marc a consulté un ami qui lui a conseillé l'achat d'un composant qui permet d'intercepter les communications entre le clavier et l'ordinateur de Valérie pour réaliser une attaque Man in the Middle.

Ce composant se configure automatiquement. Ce composant est très discret : il peut être caché dans la poche et ensuite être piloté depuis un téléphone cellulaire.

Le composant est cher et dépasse les économies que Tom a faites avec son argent de poche. En revanche, Marc a les moyens pour l'acheter.

Quelles sont les erreurs dans l'analyse de risque suivante ?

Scénario	Capacité	Opportunité	Motivation	Probabilité	Impact	Risque
C) Marc réalise une attaque MITM pour bloquer / modifier les communications entre le clavier et l'ordinateur de Valérie	3	2	3	2	4	8
D) Tom réalise une attaque MITM pour bloquer / modifier les communications entre le clavier et l'ordinateur de Valérie	4	4	4	4	4	12

- [x] a. L'opportunité dans C est trop basse ✔
- [x] b. La capacité dans C est trop basse ✔
- [x] c. La probabilité dans C est trop basse ✔
- [ ] d. La motivation dans C est trop basse

Votre réponse est correcte.

Les réponses correctes sont :
La capacité dans C est trop basse,

L'opportunité dans C est trop basse,

La probabilité dans C est trop basse

◄ INF4420A Automne 2021 Cours #7 Autorisation

Aller à...

Acétates cours - Sécurité des applications WEB ►