| | |
|---|---|
| **Commencé le** | jeudi 8 février 2024, 14:01 |
| **État** | Terminé |
| **Terminé le** | jeudi 8 février 2024, 14:58 |
| **Temps mis** | 57 min 29 s |
| **Points** | 13,00/14,00 |
| **Note** | **9,29** sur 10,00 (**92,86**%) |

**Question 1**

Correct

Note de 1,00 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**

Correct

Note de 1,00 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 correcte.

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**

Correct

Note de 1,00 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 correcte.

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**

Correct

Note de 1,00 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**

Incorrect

Note de 0,00 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 ».