Temps restant 0:06:46 Cacher

Question 1

Réponse enregistrée

Noté sur 1,00

Lesquels de ces algorithmes sont conçus pour des ordinateurs quantiques ? (plusieurs réponses possibles)

- [x] a. L'algorithme de Grover
- [ ] b. L'algorithme d'Euclide
- [x] c. L'algorithme de Shor
- [ ] d. L'algorithme de Pollard

Temps restant 0:06:13 Cacher

Question 2

Réponse enregistrée

Noté sur 2,00

Basile envoie à Anna le jour de la semaine de leur prochain rendez-vous.

Le message est chiffré avec du chiffrement par substitution mono-alphabétique.

Maxime intercepte le message chiffré qui est GKFMFKMV.

Quelle affirmation est vraie ?

- a. Anna et Basile vont se voir vendredi
- b. Maxime doit faire une attaque par analyse fréquentielle pour savoir
- c. Anna et Basile vont se voir mercredi
- d. Maxime doit faire une attaque par force brute pour savoir
- e. Anna et Basile vont se voir samedi
- f. Maxime ne peut pas déchiffrer le message

Effacer mon choix

Temps restant 0:06:03 Cacher

Question 3

Réponse enregistrée

Noté sur 1,00

Dans une infrastructure à clés publiques, quelles sont les différentes solutions pour révoquer un certificat ? (plusieurs réponses possibles)

- [x] a. Chaque certificat possède une date d'expiration. Le navigateur (browser ou butineur) du client doit vérifier que la date d'expiration n'est pas atteinte.
- [ ] b. Chaque certificat possède une date d'expiration. L'autorité de certification doit supprimer le certificat lorsque la date d'expiration est atteinte.
- [x] c. L'autorité de certification peut décider de révoquer un certificat. Le navigateur (browser ou butineur) du client doit consulter l'autorité de certification pour vérifier que le certificat n'a pas été révoqué.
- [ ] d. L'autorité de certification peut décider de révoquer un certificat. L'autorité de certification doit supprimer le certificat lorsqu'il a été révoqué.

Temps restant 0:05:54 Cacher

Question 4

Réponse enregistrée

Noté sur 2,00

Un escroc essaye d'arnaquer un club de personnes âgées. Dans un premier scénario, l'escroc envoie, aux membres de ce club, un courriel d'hameçonnage leur faisant croire qu'ils ont gagné un voyage à Acapulco. Hélas pour cet escroc, les membres de ce club ont été sensibilisés et aucun des membres ne mord à l'hameçon.

L'escroc n'abandonne pas pour autant et met au point un deuxième scénario. Il prend contact avec des membres du club en leur faisant croire qu'il est organisateur de fêtes de fin d'année. Plusieurs membres du club sont intéressés et l'escroc envoie un nouveau message d'hameçonnage pour les inviter au restaurant.

Quel facteur de risque a changé entre le premier et le second scénario ?

- a. Augmentation de la capacité
- b. Augmentation de l'impact
- c. Augmentation de la motivation
- d. Augmentation de l'opportunité

Effacer mon choix

Question 5

Réponse enregistrée

Noté sur 1,00

Utilisation d'un jeu de 32 cartes pour générer une clé de chiffrement

Dans un jeu de 32 cartes, il y a 4 enseignes : Trèfle (T), Carreau (K), Cœur (C) et Pique (P)

Les enseignes Trèfle et Pique sont noires (N). Les enseignes Carreau et Cœur sont rouges (R).

Dans chaque enseigne, il y a 8 cartes possibles : As, Roi, Dame, Valet, 10, 9, 8 et 7.

Pour générer la clé, on tire aléatoirement une carte dans le jeu.

Après chaque tirage, la carte tirée est remise dans le jeu.

On suppose que le jeu est parfaitement mélangé.

On considère 4 sources différentes pour générer la clé :

Source S1 :

- Si la carte tirée est une carte rouge, alors la source S1 génère un 0.
- Si la carte tirée est une carte noire, alors la source S1 génère un 1.

Source S2 :

- Si la carte tirée est un trèfle, alors la source S2 génère 00.
- Si la carte tirée est un carreau, alors la source S2 génère 01.
- Si la carte tirée est un cœur, alors la source S2 génère 10.
- Si la carte tirée est un pique, alors la source S2 génère 11.

Source S3 :

- Si la carte tirée est un trèfle, alors la source S3 génère 00.
- Si la carte tirée est un pique, alors la source S3 génère 01.
- Si la carte tirée est une carte rouge, alors la source S3 génère 10.

Source S4 :

- Si la carte tirée est un as, alors la source S4 génère 000.
- Si la carte tirée est un roi, alors la source S4 génère 001.
- Si la carte tirée est une dame, alors la source S4 génère 010.
- Si la carte tirée est un valet, alors la source S4 génère 011.
- Si la carte tirée est un 10, alors la source S4 génère 100.
- Si la carte tirée est un 9, alors la source S4 génère 101.
- Si la carte tirée est une 8, alors la source S4 génère 110.
- Si la carte tirée est un 7, alors la source S4 génère 111.

Quelle est l'entropie de chacune de ces sources :

S1 1

S2 1

S4 1

S3 1,5

Temps restant 0:05:40 Cacher

Question 6

Réponse enregistrée

Noté sur 1,00

Suite de la question précédente

On utilise les sources S1, S2, S3 et S4 pour générer des clés de 120 bits.

On utilise ces clés pour chiffrer un message M de longueur 120 bits en faisant un XOR entre M et la clé.

Lesquels de ces chiffrements peuvent être considérés parfaits ? (plusieurs réponses possibles)

- [x] a. Avec la clé générée par S2
- [ ] b. Avec la clé générée par S3
- [x] c. Avec la clé générée par S4
- [x] d. Avec la clé générée par S1

Temps restant 0:05:35 Cacher

Question 7

Réponse enregistrée

Noté sur 1,00

Suite de la question précédente

On suppose dans cette question qu'il manque deux cartes dans le jeu : l'as de pique et l'as de cœur.

Comme dans la question précédente, on utilise les sources S1, S2, S3 et S4 pour générer des clés de 120 bits.

On utilise ces clés pour chiffrer un message M de longueur 120 bits en faisant un XOR entre M et la clé.

Lesquels de ces chiffrements peuvent être considérés parfaits ? (plusieurs réponses possibles)

- [ ] a. Avec la clé générée par S4
- [x] b. Avec la clé générée par S1
- [ ] c. Avec la clé générée par S3
- [ ] d. Avec la clé générée par S2

Temps restant 0:05:29 Cacher

Question 8

Réponse enregistrée

Noté sur 1,00

On suppose dans cette question que le jeu ne contient plus que 16 cartes : les 8 cartes Trèfle et les 8 cartes Carreaux.

Comme dans la question précédente, on utilise les sources S1, S2, S3 et S4 pour générer des clés de 120 bits.

Quelle est l'entropie de chacune des clés ?

Clé générée par S4 60 bits

Clé générée par S3 60 bits

Clé générée par S2 60 bits

Clé générée par S1 60 bits

Temps restant 0:05:21 Cacher

Question 9

Réponse enregistrée

Noté sur 2,00

Comme dans la question précédente, on considère un jeu qui contient 16 cartes : les 8 cartes Trèfle et les 8 cartes carreaux.

On utilise les sources S1, S2, S3 et S4 pour générer des clés de 120 bits.

On utilise ces clés pour chiffrer un message M de longueur 120 bits en faisant un XOR entre M et la clé.

Lesquels de ces chiffrements peuvent être considérés parfaits ? (plusieurs réponses possibles)

- [x] a. Avec la clé générée par S1
- [x] b. Avec la clé générée par S2
- [ ] c. Avec la clé générée par S4
- [x] d. Avec la clé générée par S3

Temps restant 0:05:15 Cacher

Question 10

Réponse enregistrée

Noté sur 2,00

Utilisation d'un jeu de 32 cartes pour générer un mot de passe

Dans un jeu de 32 cartes, il y a 4 enseignes : Trèfle (T), Carreau (K), Cœur (C) et Pique (P)

Les enseignes Trèfle et Pique sont noires (N). Les enseignes Carreau et Cœur sont rouges (R).

Dans chaque enseigne, il y a 8 cartes possibles : As, Roi, Dame, Valet, 10, 9, 8 et 7.

Pour générer le mot de passe, on tire aléatoirement une carte dans le jeu.

Après chaque tirage, la carte tirée est remise dans le jeu.

On suppose que le jeu est parfaitement mélangé.

Chaque tirage permet de sélectionner un caractère du mot de passe.

La source S pour générer le mot de passe suit l'algorithme suivant :

- Si la carte tirée est le valet de pique, alors le caractère choisi est « v ».
- Sinon, si la carte tirée est un As, alors le caractère choisi est « a ».
- Sinon, si la carte tirée est un Trèfle, alors le caractère choisi est « t ».
- Sinon, si la carte tirée est un Pique, alors le caractère choisi est « p ».
- Sinon, le caractère choisi est « r ».

Par exemple, si on tire successivement les 6 cartes suivantes : 7 de trèfle, 8 de cœur, Valet de pique, As de carreau, 8 de cœur et Dame de Pique, alors le mot de passe généré est : « trvarp ».

Quelle est l'entropie caractère par caractère de la source S ?

- a. Environ 2,5
- b. Environ 1,5
- c. Environ 2,25
- d. Environ 1,25
- e. Environ 1,75
- f. Environ 2

Effacer mon choix

Temps restant 0:05:07 Cacher

Question 11

Réponse enregistrée

Noté sur 1,00

Les hypothèses sont identiques à la question précédente

On considère un mot de passe de 6 caractères.

Combien de mots de passe un attaquant doit-il tester pour avoir 100% de chance de casser le mot de passe ?

- a. 3125
- b. 46656
- c. 15625
- d. 7776

Effacer mon choix

Temps restant 0:05:01 Cacher

Question 12

Réponse enregistrée

Noté sur 2,00

Les hypothèses sont identiques à la question précédente

On considère toujours un mot de passe de 6 caractères.

On suppose que l'attaquant connait l'algorithme de génération des mots de passe et suit la meilleure stratégie possible pour casser le mot de passe.

Combien de mots de passe un attaquant doit-il tester pour avoir 5% de chance de casser le mot de passe ?

- a. Environ 100 mots de passe
- b. Environ 5 mots de passe
- c. Environ 50 mots de passe
- d. 1 seul mot de passe
- e. Environ 15 mots de passe
- f. Environ 250 mots de passe
- g. Environ 500 mots de passe

Effacer mon choix

Temps restant 0:04:56 Cacher

Question 13

Réponse enregistrée

Noté sur 1,00

L'utilisation de requêtes SQL pré-enregistrées (SQL stored procedures) dans un moteur de base de données constitue une bonne contre-mesure contre les attaques par injection SQL pour toutes ces raisons sauf :

a. Elles permettent de restreindre les droits des utilisateurs en limitant leur accès aux seules opérations autorisées via les procédures.

b. Elles permettent de paramétrer les entrées utilisateur en évitant la concaténation directe dans les requêtes SQL.

c. Elles garantissent automatiquement une validation stricte des données saisies.

d. Elles isolent les instructions SQL du code applicatif, limitant ainsi les failles exploitables par des attaquants.

Effacer mon choix

Temps restant 0:04:48 Cacher

Question 14

Réponse enregistrée

Noté sur 1,00

Vous vous connectez au site Pokéchange, le site d'échange de cartes Pokémon. Vous remarquez que l'utilisation de votre CPU augmente. En analysant la page, vous remarquez que le commentaire d'un utilisateur est une balise HTML contenant du code JavaScript qui fait du minage de cryptomonnaies.

De quelle attaque s'agit-il ?

- a. CSRF (Cross-site request forgery)
- b. Fuite de mémoire
- c. XSS (Cross-site scripting) permanent
- d. XSS (Cross-site scripting) non permanent

Effacer mon choix

Temps restant 0:04:41 Cacher

Question 15

Réponse enregistrée

Noté sur 1,00

Code vulnérable

Voici un exemple de code PHP:

```php
<?php

// Vérification si l'utilisateur est connecté
session_start();

if (!isset($_SESSION['logged_in']) || $_SESSION['logged_in'] !== true) {
    exit("Vous devez être connecté pour effectuer cette action.");
}

// Traitement de la demande de transfert d'argent
if (isset($_POST['amount']) && isset($_POST['recipient'])) {
    $amount = $_POST['amount'];
    $recipient = $_POST['recipient'];

    // Logique fictive de transfert
    echo "Transfert de $amount vers $recipient effectué avec succès.";
}

?>
```

Explication : L'instruction **isset** en PHP est une fonction booléenne qui permet de vérifier si une variable est définie et n'est pas nulle.

Pourquoi le code initial est-il vulnérable ?

- a. Il n'échappe pas les entrées utilisateur dans les champs du formulaire.
- b. Il n'utilise pas de session pour vérifier si l'utilisateur est connecté.
- c. Il accepte les requêtes POST sans vérifier leur origine ni leur authenticité.
- d. Il n'exige pas de mot de passe pour effectuer le transfert.

Effacer mon choix

Temps restant 0:04:35 Cacher

Question 16

Réponse enregistrée

Noté sur 1,00

Suite de la question précédente

Quel type d'attaque permet d'exploiter cette vulnérabilité ?

- a. XSS (Cross-site scripting) non permanent
- b. XSS (Cross-site scripting) permanent
- c. CSFR (Cross-site request forgery)
- d. Condition de course (Race condition)

Effacer mon choix

Temps restant 0:04:30 Cacher

Question 17

Réponse enregistrée

Noté sur 1,00

Suite de la question précédente

Quelle méthode permet de prévenir cette attaque ?

a. Valider l'origine de la requête en vérifiant le domaine de l'utilisateur.

b. Utiliser un jeton d'authentification unique pour chaque utilisateur et session.

c. Limiter les utilisateurs à des actions via HTTPS uniquement.

d. Utiliser des requêtes GET au lieu de POST pour les actions sensibles.

Effacer mon choix

Question 18

Réponse enregistrée

Noté sur 1,00

Code vulnérable

Scénario :

Un site de commerce électronique gère un stock de produits via un script PHP. Les utilisateurs peuvent acheter des produits en ligne, et le stock est décrémenté lorsqu'une commande est passée.

Script de gestion de stock

```php
<?php

session_start();

// Stock actuel d'un produit
$stockFile = "/tmp/product_stock.txt";

// Initialiser le stock si le fichier n'existe pas
if (!file_exists($stockFile)) {
    file_put_contents($stockFile, 0); // Stock initial : 0 unités
}

// Charger le stock actuel
$stock = (int)file_get_contents($stockFile);

if ($stock <= 0) {
    exit("Le produit est en rupture de stock.");
}

// Simuler un délai avant la mise à jour du stock
sleep(2);

// Décrémenter le stock
$stock--;

file_put_contents($stockFile, $stock);

echo "Commande passée avec succès. Stock restant : $stock\n";

?>
```

Quel est le problème principal dans le code vulnérable ?

- a. Le délai introduit par la fonction sleep() provoque des conflits.
- b. Plusieurs utilisateurs peuvent lire et modifier la valeur du stock en même temps.
- c. Le fichier contenant le stock n'est pas sécurisé.
- d. Le script ne vérifie pas si les utilisateurs sont authentifiés.

Effacer mon choix

Temps restant 0:04:06 Cacher

Question 19

Réponse enregistrée

Noté sur 1,00

Suite de la question précédente

Quel type d'attaque permet d'exploiter cette vulnérabilité ?

- a. Condition de course (Race condition)
- b. XSS (Cross-site scripting) permanent
- c. XSS (Cross-site scripting) non permanent
- d. CSFR (Cross-site request forgery)

Effacer mon choix

Temps restant 0:03:59 Cacher

Question 20

Réponse enregistrée

Noté sur 1,00

Suite de la question précédente

Quelle est la solution la plus robuste pour corriger cette vulnérabilité ?

- a. Augmenter la quantité de stock disponible.
- b. Vérifier que l'utilisateur a l'autorisation de modifier la quantité de stock.
- c. Utiliser un fichier de verrouillage pour synchroniser les accès.
- d. Ajouter un délai pour limiter les conflits.

Effacer mon choix

Question 21

Réponse enregistrée

Noté sur 2,00

Expression de la politique d'autorisation d'une entreprise

Vous venez d'être embauché comme administrateur de la sécurité dans l'entreprise NOZAMA.

Votre première mission consiste à définir la politique d'autorisation de cette entreprise.

Vous décidez d'utiliser le modèle AGLP (Access – Global – Local – Permissions).

Cette entreprise possède deux filiales : NOZAMA Canada (NC) et NOZAMA France (NF).

L'ensemble R des rôles (groupes globaux du modèle AGLP) est le suivant :

R = {Developpeur, Gestionnaire, Auditeur, Developpeur_NC, Developpeur_NF, Admin_projet, Admin_facturation}

Le but de la politique d'autorisation est de contrôler l'accès à des dossiers des patients.

- L'ensemble des types de ressources (groupes locaux du modèle AGLP) est le suivant : G = {Projet_NOZAMA, Projet_NC, Projet_NF, Facturation}
- L'ensemble des actions qu'il est possible de réaliser sur les ressources est le suivant : A = {Créer, Lire, Modifier}
- Le rôle Developpeur_NC peut lire et modifier les ressources Projet_NC.
- Le rôle Developpeur_NF peut lire et modifier les ressources Projet_NF.
- Le rôle Developpeur peut lire et modifier les ressources Projet_NOZAMA
- Les Developpeur_NC et Developpeur_NF sont des développeurs.
- Le rôle Gestionnaire peut créer et lire des ressources de Projet_NOZAMA, Projet_NC et Projet_NF. Le rôle Gestionnaire peut aussi lire et modifier les ressources de Facturation.
- Le rôle Auditeur peut lire les ressources de Projet_NOZAMA, Projet_NC, Projet_NF et Facturation.
- Le rôle Admin_projet peut lire et écrire les ressources de Projet_NOZAMA, Projet_NC, Projet_NF
- Le rôle Admin_facturation peut créer, lire et écrire les ressources de Facturation

Vous devez définir la hiérarchie de rôles. On rappelle que si le rôle A est hiérarchiquement inférieur à B, alors B hérite des permissions de A.

Remarque importante : on suppose que la hiérarchie est une relation transitive : si le rôle A est hiérarchiquement inférieur à B et si B est hiérarchiquement inférieur à C alors A est hiérarchiquement inférieur à C.

< Developpeur_NF, Admin_projet >	Hiérarchiquement inférieur
< Gestionnaire, Developpeur_NF >	Incomparable
< Developpeur_NC, Developpeur_NF >	Incomparable
< Gestionnaire, Auditeur >	Hiérarchiquement supérieur
< Developpeur, Gestionnaire >	Incomparable
< Developpeur, Developpeur_NF >	Hiérarchiquement inférieur
< Auditeur, Developpeur_NC >	Incomparable
< Developpeur, Developpeur_NC >	Hiérarchiquement inférieur
< Developpeur, Admin_projet >	Hiérarchiquement inférieur
< Admin_projet, Admin_facturation >	Incomparable
< Developpeur_NF, Admin_facturation >	Incomparable
< Developpeur, Admin_facturation >	Incomparable

< Gestionnaire, Admin_projet >	Incomparable
< Auditeur, Admin_facturation >	Incomparable
< Gestionnaire, Admin_facturation >	Incomparable
< Developpeur_NC, Admin_projet >	Hiérarchiquement inférieur
< Gestionnaire, Developpeur_NC >	Incomparable
< Developpeur, Auditeur >	Incomparable
< Developpeur_NC, Admin_facturation >	Incomparable
< Auditeur, Developpeur_NF >	Incomparable
< Auditeur, Admin_projet >	Incomparable

Temps restant 0:03:44 Cacher

Question 22

Réponse enregistrée

Noté sur 2,00

Dans cette question, il s'agit de compléter la matrice de contrôle d'accès entre les rôles et les groupes locaux de l'entreprise MOZANA.

	Projet_NOZAMA	Projet_NC	Projet_NF	Facturation
Developpeur	Case 1 ?			
Gestionnaire		Case 2 ?		Case 3 ?
Auditeur		Case 4 ?		Case 5 ?
Developpeur_NC		Case 6 ?		
Developpeur_NF				
Admin_projet		Case 7 ?		
Admin_facturation				Case 8 ?

Indiquer quelles sont les permissions dans l'ensemble A= {Créer, Lire, Modifier} pour les cases de la matrice de 1 à 8.

Important : ne pas affecter une permission à un rôle si ce rôle hérite déjà de cette permission d'un rôle hiérarchiquement inférieur.

Case 2 {Créer, Lire}

Case 5 {Lire}

Case 4 {Lire}

Case 6 {Lire, Modifier}

Case 7 {Lire, Modifier}

Case 3 {Modifier}

Case 8 {Créer, Lire, Modifier}

Case 1 {Lire, Modifier}

Temps restant 0:03:39 Cacher

Question 23

Réponse enregistrée

Noté sur 1,00

L'entreprise NOZAMA souhaite ajouter la contrainte suivante : un employé ne peut cumuler les rôles de Développeur et Auditeur.

Comment proposeriez-vous de prendre en compte cette contrainte ?

- a. Il est impossible d'ajouter cette contrainte car les rôles Développeur et Auditeur peuvent tous les deux lire le Projet_NOZAMA.
- b. Une contrainte de séparation des pouvoirs statique (SSOD) entre les rôles Développeur et Auditeur.
- c. Il n'y a pas besoin d'ajouter de contrainte : dans le modèle AGLP, un utilisateur ne peut être affecté qu'à un seul rôle.
- d. Une contrainte de séparation des pouvoirs dynamique (DSOD) entre les rôles Développeur et Auditeur.

Effacer mon choix

Temps restant 0:03:33 Cacher

Question 24

Réponse enregistrée

Noté sur 1,00

L'entreprise NOZAMA souhaite ajouter la contrainte suivante : un employé ne peut activer en même temps les rôles Admin_projet et Admin_facturation.

Comment proposeriez-vous de prendre en compte cette contrainte ?

a. Il est impossible d'exprimer cette contrainte avec le modèle AGLP.

b. Une contrainte de séparation des pouvoirs dynamique (DSOD) entre les rôles Admin_projet et Admin_facturation.

c. Une contrainte de séparation des pouvoirs statique (SSOD) entre les rôles Admin_projet et Admin_facturation.

d. Il n'y a pas besoin d'ajouter de contrainte : dans le modèle AGLP, un utilisateur ne peut activer qu'un seul rôle à la fois.

Effacer mon choix

Temps restant 0:03:28 Cacher

Question 25

Réponse enregistrée

Noté sur 2,00

Alice est une employée de l'entreprise NOZAMA affectée au rôle Admin_facturation.

Alice a besoin d'argent. Elle décide de récupérer les données de Projet_NC et de les revendre à un concurrent de NOZAMA.

Pour cela, Alice a conçu une application piégée qui permet de lire les données de Projet_NC et de les recopier dans un fichier auquel elle a accès.

Alice a ensuite installé cette application sur le compte de Bob et elle attend que Bob exécute cette application.

Quel devrait être le rôle de Bob dans l'entreprise NOZAMA pour que l'attaque d'Alice réussisse ?

- a. Developpeur_NC
- b. Gestionnaire
- c. Auditeur
- d. Admin_projet
- e. Aucune de ces réponses ne permet à Alice de récupérer les données de Projet_NC

Effacer mon choix

Temps restant 0:03:23 Cacher

Question 26

Réponse enregistrée

Noté sur 1,00

Lorsqu'un attaquant A effectue une attaque "Smurf" sur un serveur B, quelles affirmations sont vraies ? (plusieurs réponses possibles)

- [ ] a. A réalise une attaque contre le protocole UDP
- [x] b. A forge des paquets ayant pour adresse destination l'adresse IP de B
- [ ] c. A forge des paquets ayant pour adresse source l'adresse IP de B
- [x] d. A effectue une attaque par inondation sur B (flooding)

Temps restant 0:03:18 Cacher

Question 27

Réponse enregistrée

Noté sur 1,00

Sous Netfilter, lorsque la chaine POSTROUTING est utilisée, laquelle de ces affirmations est vraie :

- a. Le pare-feu applique le transfert d'adresse sur l'adresse source du paquet
- b. Le pare-feu applique le transfert d'adresse sur l'adresse destination du paquet
- c. Le pare-feu applique le transfert d'adresse sur l'adresse source du paquet ET sur l'adresse destination du paquet
- d. Aucune de ces réponses : Netfilter ne gère pas le transfert d'adresse

Effacer mon choix

Temps restant 0:03:11 Cacher

Question 28

Réponse enregistrée

Noté sur 2,00

Configuration d'un pare-feu NetFilter/IPTables : Question 1

Une entreprise souhaite donner l'accès à un serveur Web via HTTPS (port 443).

Le serveur Web est sur le réseau local de l'entreprise à l'adresse privée 192.168.1.10

L'accès à ce serveur est filtré par un pare-feu Netfilter. Le pare-feu a deux interfaces réseau :

- eth0 à l'adresse publique 155.140.140.1
- eth1 à l'adresse privée 192.168.1.1

Vous devez configurer ce pare-feu pour donner accès au serveur Web.

Les règles sont les suivantes :

Règle 1 :

iptables -A OUTPUT -i eth0 -o eth1 -p tcp --dport 443 -m state --state NEW, ESTABLISHED -j ACCEPT

Règle 2 :

iptables -A FORWARD -i eth1 -o eth0 –s 192.168.1.10 –sport 443 -m state --state NEW -j ACCEPT

Règle 3 :

iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 443 -m state --state NEW, ESTABLISHED -j ACCEPT

Règle 4 :

iptables -t nat -A POSTROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.10:443

Règle 5 :

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.10:443

Règle 6 :

iptables -A FORWARD -i eth1 -o eth0 -m state --state ESTABLISHED -j ACCEPT

Indiquez les règles IPTables qui sont correctes :

Règle 4 Incorrect

Règle 5 Correct

Règle 1 Incorrect

Règle 6 Incorrect

Règle 3 Correct

Règle 2 Incorrect

Temps restant 0:03:05 Cacher

Question 29

Réponse enregistrée

Noté sur 2,00

Configuration d'un pare-feu NetFilter/IPTables : Question 2

Une entreprise souhaite donner l'accès à un serveur DNS (port 53).

Le serveur DNS doit être accessible via les protocoles UDP ou TCP.

Le serveur DNS est sur le réseau local de l'entreprise à l'adresse privée 192.168.1.100

L'accès à ce serveur est filtré par un pare-feu Netfilter. Le pare-feu a deux interfaces réseau :

- eth0 à l'adresse publique 155.140.140.1
- eth1 à l'adresse privée 192.168.1.1

Vous devez configurer ce pare-feu pour donner accès au serveur Web.

Indiquez les règles IPTables qui sont correctes :

Règle 7 :

iptables -t nat -A PREROUTING -i eth0 -p udp --dport 53 -j DNAT --to-destination 192.168.1.100:53

Règle 8 :

iptables -t nat -A POSTROUTING -i eth1 -p tcp --sport 53 -j MASCARADE

Règle 9 :

iptables -A FORWARD -i eth0 -o eth1 -p udp -m state --state NEW, ESTABLISHED -j ACCEPT

Règle 10 :

iptables -A FORWARD -i eth1 -o eth0 -p udp -m state --state RELATED -j ACCEPT

Règle 11 :

iptables -A FORWARD -i eth1 -o eth0 -p tcp -m state --state RELATED -j ACCEPT

Règle 12 :

iptables -A FORWARD -i eth0 -o eth1 -p udp --dport 53 -d 192.168.1.100 -m state --state RELATED -j ACCEPT

Règle 8	Incorrect
Règle 12	Correct
Règle 11	Incorrect
Règle 9	Correct
Règle 7	Correct
Règle 10	Incorrect

Temps restant 0:02:58 Cacher

Question 30

Réponse enregistrée

Noté sur 1,00

Soit la requête SQL suivante :

select * from table_users where login='admin' --' and pass='$_POST["pass"]'

Quel est le résultat de son exécution ?

a. L'exécution échoue, la requête est mal formatée.

b. L'exécution réussit car la requête est bien formatée, mais le pirate n'accèdera à rien.

c. Ceci n'est pas une requête SQL.

d. Si un tel login existe dans la base de données alors le pirate sera authentifié et accédera à l'espace admin.

Effacer mon choix