

[Tableau de bord](#) / Mes cours / [INF4420A - Sécurité informatique](#) / Automne 2021 Examen Final INF4420A / [Automne 2021 Examen Final](#)

Commencé le jeudi 23 décembre 2021, 09:30

État Terminé

Terminé le jeudi 23 décembre 2021, 12:00

Temps mis 2 heures 29 min

Points 33,50/40,00

Note 8,38 sur 10,00 (84%)

Question 1

Correct

Note de 1,00 sur 1,00

Sécurité logiciel Question 1

Vous voulez utiliser le mécanisme de protection reposant sur la gestion dynamique de la mémoire (ASLR). Quand est-ce que ce mécanisme est-il introduit pour protéger l'exécution du programme :

- a. Dynamiquement, quand le programme est exécuté
- b. Systématiquement, ce mécanisme est désormais natif dans la plupart des systèmes d'exploitation ✓
- c. Automatiquement, quand le programme est compilé
- d. Manuellement, quand le programmeur écrit le programme

Votre réponse est correcte.

La réponse correcte est :

Systématiquement, ce mécanisme est désormais natif dans la plupart des systèmes d'exploitation

Question 2

Correct

Note de 1,00 sur 1,00

Sécurité logiciel Question 2

Vous voulez utiliser le mécanisme de protection reposant sur les **canaries**. Quand est-ce que ce mécanisme est-il introduit pour protéger l'exécution du programme :

- a. Systématiquement, ce mécanisme est désormais natif dans la plupart des systèmes d'exploitation
- b. Automatiquement, quand le programme est compilé
- c. Dynamiquement, quand le programme est exécuté
- d. Manuellement, quand le programmeur écrit le programme

Votre réponse est correcte.

La réponse correcte est :

Automatiquement, quand le programme est compilé

Question 3

Correct

Note de 1,00 sur 1,00

Sécurité logiciel Question 3

La création d'un "shell code" qui peut être utilisé dans une attaque par débordement de tampon sur une application vulnérable est difficile.

Laquelle des propositions suivantes n'est pas une raison de ces difficultés.

- a. La distance entre le début du tampon et le pointeur de retour n'est pas toujours la même car l'exécution du programme n'est pas déterministe
- b. Le shell code doit rester suffisamment petit afin de pouvoir rentrer dans son entièreté dans le buffer et l'espace entre celui-ci et le pointeur de retour
- c. L'utilisation de NOP sled (chaîne de plusieurs 0x90) est problématique car elle peut facilement être détectée par un IDS ou autre produit de sécurité
- d. Il faut éviter que le shell code contienne des caractères NULL (0x00) qui pourraient facilement être détectés par des IDS ou autres types d'outils de sécurité informatique

Votre réponse est correcte.

La réponse correcte est :

Il faut éviter que le shell code contienne des caractères NULL (0x00) qui pourraient facilement être détectés par des IDS ou autres types d'outils de sécurité informatique

Question 4

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 :

- a. `login : « 1234 » / pwd : « blabla OR 1=1 »`
- b. `login: « 1234 » / pwd: « blabla') OR (1=1 »`
- c. `login: « 1234 » / pwd: « blabla') OR (1=1 OR pwd = ' »`
- d. `login: « 1234 » / pwd: « blabla' OR 1=1) AND (pwd=' ; »`

↓ ↓ ↓

**put another () so when (... AND ...) fails
it passes with the 1=1**

**login 1234 est un ou des vrai users
le reste est pour faire tester le pwd
a vrai toujours**

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 = '') ;`

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

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

Requête bien formée et WHERE évalué à faux = authentification refusée

La réponse correcte est :

`login: « 1234 » / pwd: « blabla') OR (1=1 OR pwd = ' »`

Question 5

Correct

Note de 1,00 sur 1,00

Injection SQL Question 2

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 :

Indication : le double tiret « `--` » permet d'insérer des commentaires en SQL.

- a. login: « `1234 OR 1 = 1` ; `--` » / pwd: « `blabla` »
- b. login: « `1234` » / pwd: « `blabla'` OR `1=1` ; `--` »
- c. login: « `1234 OR 1 = 1` » / pwd: « `blabla'` OR `1=1` ; `--` »
- d. les trois réponses ci-dessus permettent de contourner l'authentification

Dans tous les cas on ne vérifie plus le champ pwd car c'est considéré comme un commentaire



Votre réponse est correcte.

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

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

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

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

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

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

La réponse correcte est :

les trois réponses ci-dessus permettent de contourner l'authentification

Question 6

Terminer

Note de 1,00 sur 1,00

Injection SQL Question 2b

Justifier la réponse que vous avez donnée à la question "Injection SQL Question 2".

Les requêtes résultantes sont:

- a.) `SELECT * FROM users WHERE (login=1234 OR 1 = 1) ; -- AND pwd=blabla)` ;
- b.) `SELECT * FROM users WHERE (login=1234 AND pwd='blabla') OR 1=1 ; --'` ;
- c.) `SELECT * FROM users WHERE (login=1234 OR 1 = 1) AND pwd='blabla' OR 1=1 ; --'` ;

On conclut alors qu'elle marche tous, la condition va être true pour les 3 requêtes.

Commentaire :

Question 7

Correct

Note de 1,00 sur 1,00

Injection SQL Question 3**Dans le pire des cas, quelle est la portée d'une attaque par injection SQL sur une table d'une base de données relationnelle ?**

- a. La table visée
 - b. La table visée et la base de données
 - c. La table visée, la base de données et le système de gestion de base de données (SGBD) qui gère la table
 - d. La table visée, la base de données, le SGBD et le serveur qui héberge la base de données
- ✓

Votre réponse est correcte.**La réponse correcte est :**

La table visée, la base de données, le SGBD et le serveur qui héberge la base de données

Question 8

Correct

Note de 1,00 sur 1,00

Injection SQL Question 4**Vous décidez de déployer un proxy web pour intercepter les requêtes envoyées au serveur qui héberge le SGBD. Quelles règles permettront d'empêcher les attaques de type injection SQL ?**

- a. Vérifier que la requête ne contient pas de chaîne de caractères correspondant à une expression régulière de la forme « \d = \d » où \d est un chiffre
 - b. Vérifier que la requête ne contient pas de chaîne de caractères « -- »
 - c. Vérifier que les mots de passe transmis dans la requête ont été chiffrés
 - d. Vérifier que la requête ne contient pas de chaîne de caractères « 1 = 1 »
- 

Votre réponse est correcte.

Chiffrer le mot passe transmis dans la requête est une protection nécessaire mais qui ne suffit pas à protéger contre les attaques par injection SQL.

Les autres réponses sont correctes.

Les réponses correctes sont :

Vérifier que la requête ne contient pas de chaîne de caractères « 1 = 1 »,

Vérifier que la requête ne contient pas de chaîne de caractères correspondant à une expression régulière de la forme « \d = \d » où \d est un chiffre,

Vérifier que la requête ne contient pas de chaîne de caractères « -- »

Question 9

Correct

Note de 1,00 sur 1,00

Sécurité Web Question 1

Vous faites appel à la page `get_nom.php` avec en paramètre `nom=Max` :

`http://155.0.1.1/get_nom.php?nom=Max`

Dans la page `get_nom.php`, le code suivant est exécuté :

```
<?php  
echo $_GET['nom'];  
?>
```

Et affiche :

Max

Maintenant, vous remplacez Max par :

`<script>alert('Cool !')</script>`

La page `get_nom.php` ouvre une pop-up affichant "Cool!".

Quel type d'attaque venez-vous de réaliser :

- a. Débordement de pile (stack overflow)
- b. CSRF (Cross Site Request Forgery)
- c. Cross Site Scripting (XSS) non permanent
- d. Cross Site Scripting (XSS) permanent



Votre réponse est correcte.

La réponse correcte est :

Cross Site Scripting (XSS) non permanent

Question 10

Correct

Note de 1,00 sur 1,00

Entropie Question 1

On considère une source S1 markovienne qui génère des 0 et des 1. La probabilité d'apparition d'un 0 est de $\frac{1}{4}$ et celle d'un 1 est de $\frac{3}{4}$. Quelle est l'entropie d'un message de 10 chiffres généré par la source S1 ?

- a. 8,11
- b. 0,811
- c. 10
- d. 5

pour 1 caractère
 $1/4 \cdot \log_2(4) + 3/4 \cdot \log_2(4/3) = 0.811278$

le message de 10 chiffres
 $0.811278 \cdot 10 = 8.11$



Votre réponse est correcte.

La réponse correcte est :

8,11

Question 11

Correct

Note de 1,00 sur 1,00

XOR si même bit => 0**Entropie Question 2**

On considère une seconde source S2 markovienne qui génère également des 0 et des 1. La probabilité d'apparition d'un 0 est de $\frac{1}{2}$ et celle d'un 1 est de $\frac{1}{2}$.

La source S est obtenue en prenant le XOR (OU exclusif) des bits générés par S1 et S2.

Quelle est l'entropie d'un message de 10 chiffres généré par la source S ?

- a. 8,11
- b. 0,811
- c. 5
- d. 10

$p(s1=0)=1/4$
 $p(s1=1)=3/4$
 $p(s2=0)=1/2$
 $p(s2=1)=1/2$

s1	s2	s
0	0	0
0	1	1
1	0	1
1	1	1

pour s=1
soit s1=0, s2=1
ou s1=1, s2=0

$p(s1=0 \text{ et } s2=1)=1/4 \cdot 1/2=1/8$
 $p(s1=1 \text{ et } s2=0)=3/4 \cdot 1/2=3/8$
 $p(s=1)=1/8+3/8=1/2$

Votre réponse est correcte.

La réponse correcte est :

10

$p(s1=0 \text{ et } s2=0)=1/4 \cdot 1/2=1/8$
 $p(s1=1 \text{ et } s2=1)=3/4 \cdot 1/2=3/8$
 $p(s=0)=1/8+3/8=1/2$

$E=1/2 \cdot \log_2(2)+1/2 \cdot \log_2(2)=1$ pour 1 caractère
 $1 \cdot 10 = 10$ bits pour 10 caractères

Question 12

Correct

Note de 1,00 sur 1,00

Entropie Question 3

Dans la question précédente, on suppose que la source S2 sert à générer une clé de chiffrement. Et on suppose que S1 est le message à chiffrer.

On peut considérer que le chiffrement est parfait.

si clé aussi long que message
=> parfait

Sélectionnez une réponse :

Vrai

Faux

chaque caractère est équiprobable pour la clé
1/2 pour 0 et 1/2 pour 1
on a juste 2 choix possibles dans l'alphabet

La réponse correcte est « Vrai ».

pour s2
1 caractère
 $1/2 \cdot \log_2(2) + 1/2 \cdot \log_2(2) = 1$
s1 génère 0 ou 1
donc la longueur du message est 1 aussi

Question 13

Correct

Note de 1,00 sur 1,00

Entropie Question 4

On considère une troisième source S3 markovienne qui génère des 0 et des 1. La probabilité d'apparition d'un 0 et de 1/3 et celle d'un 1 est de 2/3.

La source S' est obtenue en prenant le XOR (OU exclusif) des bits générés par S1 et S3.

Quelle est l'entropie d'un message de 10 chiffres généré par la source S' ?

- a. 8,95
- b. 6,67
- c. 9,80
- d. 10

s1	s2	s
0	0	0
0	1	1
1	0	1
1	1	1



pour que s=0

soit s1=0, s3=0
ou s1=1, s3=1

$$p(s1=0 \text{ et } s3=0) = 1/4 \cdot 1/3 = 1/12$$

$$p(s1=1 \text{ et } s3=1) = 3/4 \cdot 2/3 = 1/2$$

$$p(s=0) = 1/12 + 1/2 = 7/12$$

pour que s=1

soit s1=0 et s3=1
ou s1=1 et s3=0

$$p(s1=0 \text{ et } s3=1) = 1/4 \cdot 2/3 = 1/6$$

$$p(s1=1 \text{ et } s3=0) = 3/4 \cdot 1/3 = 1/4$$

$$p(s=1) = 1/6 + 1/4 = 5/12$$

Votre réponse est correcte.

Probabilité d'apparition de 1 : $1/4 \cdot 2/3 + 3/4 \cdot 1/3 = 2/12 + 3/12 = 5/12$

Probabilité d'apparition de 0 : $1/4 \cdot 1/3 + 3/4 \cdot 2/3 = 1/12 + 6/12 = 7/12$

$$E' = 5/12 \cdot \log_2(12/5) + 7/12 \cdot \log_2(12/7) = 5/12 \cdot 1.26303 + 7/12 \cdot 0.777608 = 0,98$$

Entropie d'un message de 10 chiffres généré par la source S' = $0,980 \cdot 10 = 9,80$

La réponse correcte est :

9,80

$E=7/12 \cdot \log_2(12/7) + 5/12 \cdot \log_2(12/5) = 0.979868$ pour 1 caractère
 $0.979868 \cdot 10 = 9.80$ pour 10 caractères

Question 14

Correct

Note de 1,00 sur 1,00

Entropie Question 5On considère la source S'' est obtenue en prenant le ET logique des bits générés par S_1 et S_3 .

pour $s=0$
 soit $s_1=0, s_3=0$
 ou $s_1=0, s_3=1$
 ou $s_1=1, s_3=0$

Quelle est l'entropie d'un message de 10 chiffres généré par la source S'' ?

- a. 10
- b. 6,67
- c. 9,80
- d. 8,95

	$p(s_1=0)=1/4$	s_1	s_3	s
	$p(s_1=1)=3/4$	0	0	0
		0	1	0
		1	0	0
		1	1	1
	$p(s_3=0)=1/3$			
	$p(s_3=1)=2/3$			

$$\begin{aligned}
 p(s_1=0 \text{ et } s_3=0) &= 1/4 * 1/3 = 1/12 \\
 p(s_1=0 \text{ et } s_3=1) &= 1/4 * 2/3 = 1/6 \\
 p(s_1=1 \text{ et } s_3=0) &= 3/4 * 1/3 = 1/4 \\
 p(s=0) &= 1/12 + 1/6 + 1/4 = 1/2 \\
 &\quad \text{pour } s=1 \\
 &\quad s_1=1, s_3=1 \\
 p(s_1=1 \text{ et } s_3=1) &= 3/4 * 2/3 = 1/2 \\
 p(s=1) &= 1/2
 \end{aligned}$$

$$E = 1/2 \log(2) + 1/2 \log(2) = 1 \text{ pour 1 caractère}$$

10 pour 10 caractère

Votre réponse est correcte.

- Probabilité d'apparition de 0 : $1/4 * 2/3 + 3/4 * 1/3 + 1/4 * 1/3 = 2/12 + 3/12 + 1/12 = 1/2$
- Probabilité d'apparition de 1 : $3/4 * 2/3 = 6/12 = 1/2$

$$E' = 1/2 + 1/2 = 1$$

Entropie d'un message de 10 chiffres généré par la source $S' = 1 * 10 = 10$ bits

La réponse correcte est :

10

Question 15[Terminer](#)

Note de 2,00 sur 2,00

Entropie Question 6

Dans la question précédente, on suppose que la source S_3 sert à générer une clé de chiffrement. Et on suppose que S_1 est le message à chiffrer.

Peut-on considérer que le chiffrement est parfait ?

Justifier votre réponse.

Ce chiffrement nous donne l'entropie maximale, tout comme le chiffrement de la Question2, qui est d'ailleurs (le chiffrement de Q2) le chiffrement par masque jetable. Comme la clé de ce chiffrement (celui de Q2) est parfaitement aléatoire, d'après Shannon, la source S (question 2) donne un chiffrement parfait.

Cependant ici, la clé n'est pas parfaitement aléatoire, elle génère 0 dans 1/3 de cas et 1 dans 2/3 de cas. Le chiffrement ici n'est pas parfait. D'ailleurs si on change la source de message à chiffrer S_1 en changeant son entropie, on arriverait plus à une entropie maximale. Alors que dans le cas du chiffrement avec XOR (Q2), on arriverait toujours à une entropie maximale (la preuve mathématique est assez simple, on pose p et $1-p$ la probabilité de 0 et 1 pour le message et on refait l'arbre de probabilités)

Bien que l'entropie du résultat généré par S'' soit maximal, le chiffrement n'est pas parfait.

En effet, si un "1" est présent dans le résultat en position i , alors on peut déduire que le message à chiffrer contient un "1" en position i et aussi que la clé contient un "1" en position i .

Réponse également acceptée : l'entropie de la clé n'est pas maximale.

Et aussi : Le seul chiffrement parfait (chiffrement de Vernam) repose sur l'opération logique XOR

Commentaire :

Question 16

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 1

La translation d'adresses sert à :

- a. Cacher les adresses publiques
- b. Gérer la pénurie d'adresses
- c. Sécuriser le proxy
- d. Augmenter le nombre d'adresses publiques



Votre réponse est correcte.

La réponse correcte est :

Gérer la pénurie d'adresses

Question 17

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 2

Configuration d'un pare-feu Netfilter

On considère la configuration suivante d'un pare-feu Netfilter :

```
# set default closed policy
iptables -P FORWARD DROP

# network interfaces
EXTIF=eth0
INTIF=eth2
on prend 192.168.4.0+1
et 192.168.4.255-1
comme limite des IP dans ce réseau

# addresses
192.168.4.1 à 192.168.4.254
EXTIP=195.55.55.1
EMP_HOST=192.168.4.0/24

# enable SNAT (MASQUERADE) functionality on External interface
iptables -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE

# EMP must be able to access Internet
iptables -A FORWARD -i $INTIF -o $EXTIF -s $EMP_HOST -dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i $INTIF -o $EXTIF -s $EMP_HOST -dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i $INTIF -o $EXTIF -s $EMP_HOST -dport 53 -m state --state RELATED -j ACCEPT
```

On considère que les paquets suivants arrivent, dans cet ordre, sur l'interface INTIF du firewall NetFilter (on suppose que le pare-feu n'a pas reçu de paquet avant Packet#1) :

Packet	Protocole	Src-IP	Dest-IP	Src-Port	Dest-Port	TCP Flags		
						SYN	SYN-ACK	ACK
Packet#1	TCP	192.168.1.1	195.5.5.1	2240	80	1	0	0
Packet#2	TCP	192.168.4.1	195.5.5.1	2240	80	1	0	0
Packet#3	TCP	195.5.5.1	195.55.55.1	80	1030	0	1	0
Packet#4	TCP	195.5.5.1	195.55.55.1	80	1035	0	1	0
Packet#5	TCP	192.168.4.1	195.5.5.1	2240	80	0	0	1

Packet	Protocole	Src-IP	Dest-IP	Src-Port	Dest-Port
Packet#6	UDP	192.168.4.1	195.5.5.2	3535	53
Packet#7	UDP	195.5.5.2	195.55.55.1	53	1040

Packet	Protocole	Src-IP	Dest-IP	TYPE	CODE	Payload attributes			
						Src-IP	Dest-IP	Src-Port	Dest-Port

Packet#8	ICMP	195.5.5.2	195.55.55.13	3	195.55.55.1	195.5.5.2	1040	53
----------	------	-----------	--------------	---	-------------	-----------	------	----

Laquelle de ces affirmations est vraie ?

- a. Le pare-feu bloque le Packet#1 et accepte le Packet#2
- b. Le pare-feu bloque le Packet#1 et le Packet#2
- c. Le pare-feu accepte le Packet#1 et le Packet#2
- d. Le pare-feu accepte le Packet#1 et bloque le Packet#2

192.168.1.1 n'est pas dans l'intervalle 192.168.4.1 à 192.168.4.254 donc rejeté tandis que 192.168.4.1 dedans donc ok ✓

Votre réponse est correcte.

La réponse correcte est :

Le pare-feu bloque le Packet#1 et accepte le Packet#2

Question 18

Terminer

Note de 2,00 sur 2,00

Sécurité réseau Question 3

On suppose que le pare-feu accepte le Packet#3. Faites les hypothèses qui correspondent à cette situation. **Donner la table de translation.**

Le parefeu accepte le Packet#3 car c'est le serveur http de l'adresse 195.5.5.1 qui répond avec un SYN-ACK à l'employé 192.168.4.1. En effet, l'employé a envoyé du port source 2240 mais le NAT a fait la translation de port avant d'envoyer le ACK (il l'a translaté au port 1030) au serveur à 195.5.5.1

Prenons comme hypothèse que la table de translation est la suivante:

IP publique	Port publique	IP public	Port privé
195.55.55.1	1030	192.168.4.1	2240

ACK la réponse et NAT a translaté au port destination 1030

192.168.4.1 port 1030 195.5.5.1 port 2240

packet 3 est un syn-ack donc packet 2 est un syn

Le Packet#3 est un message SYN-ACK envoyé par le serveur web d'adresse IP 195.5.5.1.

Si le Packet#3 est accepté par le pare-feu, cela signifie qu'il s'agit de la réponse à la demande de connexion (paquet SYN) correspondant au Packet#2.

La table de translation est donc la suivante :

IP privée : 192.168.4.1 --> IP publique : 195.5.5.1

Port privé : 2240 --> Port public : 1030

Commentaire :

Question 19

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 4

On suppose que le pare-feu accepte le Packet#3. La pare-feu va aussi accepter le Packet#4.

Sélectionnez une réponse :

- Vrai
 Faux

port dest correspond
à aucune demande
client seul port client
connu est 1030 qui a
fait demande de
connection via SYN

Le Packet#4 sera refusé car le port destination ne correspond à aucune demande de connexion côté client (compte tenu des hypothèses faites à question précédente).

La réponse correcte est « Faux ».

Question 20

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 5

À la fin de la séquence de paquets Packet#1-Packet#5, la table de session du pare-feu contiendra l'entrée suivante :

Connection	Protocol	Src-IP	Dest-IP	Src-Port	Dest-Port	Connection State	Timeout
Connection#1	TCP	192.168.4.1	195.5.5.1	2240	53 1030	Established Full connection Default	3600s

Sélectionnez une réponse :

- Vrai
 Faux

La réponse correcte est « Faux ».

Question 21

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 6**Le pare-feu accepte le paquet Packet#6****Sélectionnez une réponse :** Vraimême IP source et le port UDP
défini comme related Faux

La réponse correcte est « Vrai ».

Question 22

Incorrect

Note de 0,00 sur 1,00

Sécurité réseau Question 7**On suppose que le pare-feu accepte le paquet Packet#7. Que va faire le pare-feu quand il va recevoir le paquet Packet#8 ?**

- a. Le pare-feu va créer une nouvelle entrée dans sa table de session
- b. Le paquet va être bloqué ✗
- c. Le pare-feu va générer un paquet ICMP et l'envoyer à l'adresse IP 155.5.5.2 sur le port 53
- d. **Le pare-feu va accepter le paquet et le transférer à l'adresse IP 192.168.4.1 sur le port 3535**

Votre réponse est incorrecte.

Le pare-feu va considérer que le paquet Packet#8 est un message d'erreur envoyé par le serveur DNS à qui a été envoyé une demande dans le Packet#6 par la machine à l'adresse privée IP 192.168.4.1.

Le pare-feu va donc transférer ce message ICMP à l'adresse privée IP 192.168.4.1 sur le port 3535.

La réponse correcte est :

Le pare-feu va accepter le paquet et le transférer à l'adresse IP 192.168.4.1 sur le port 3535

Question 23

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 8

Vous constatez que le pare-feu reçoit un grand nombre de paquets semblables au Packet#8. A quel type d'attaque cela vous fait-il penser ?

- a. Syn-Flooding
- b. Slow Loris
- c. Black Nurse
- d. Smurf



Votre réponse est correcte.

La réponse correcte est :

Black Nurse

Question 24

Incorrect

Note de 0,00 sur 1,00

Autorisation Question 1

Expression de la politique d'autorisation d'un hôpital.

Vous venez d'être embauché comme administrateur de la sécurité dans un hôpital.

Votre première mission consiste à définir la politique d'autorisation de cet hôpital.

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

Cet hôpital comprend 3 services : radiologie, pédiatrie et ophtalmologie.

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

$R = \{\text{Médecin, Radiologue, Pédiatre, Ophtalmologue, Stagiaire_radiologue, Stagiaire_pédiatre, Stagiaire_ophtalmologue, Infirmier}\}$

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 : $G = \{\text{Dossier_patient_radiologie, Dossier_patient_pédiatrie, Dossier_patient_ophtalmologie}\}$
- L'ensemble des actions qu'il est possible de réaliser sur les ressources est le suivant : $A = \{\text{Créer, Lire, Modifier}\}$
- **Les radiologues, les pédiatres, les ophtalmologues sont des médecins.**
- Les pédiatres sont affectés au service de pédiatrie.
- Les radiologues sont affectés au service de radiologie.
- Les ophtalmologues sont affectés au service ophtalmologie.
- Les médecins peuvent lire tous les dossiers médicaux. En revanche, un médecin ne peut créer ou modifier le dossier d'un patient que si ce dossier est dans le même service que le médecin.
- Les stagiaires en radiologie, pédiatrie et ophtalmologie sont respectivement affectés aux services de radiologie, pédiatrie et ophtalmologie. Les stagiaires sont des apprentis médecins. Ils sont sous l'autorité d'un médecin du service dans lequel ils sont affectés.
< radiologue
- Un stagiaire peut créer ou lire le dossier d'un patient qui est dans le même service que celui dans lequel le stagiaire est affecté. En revanche, un stagiaire ne peut pas modifier le dossier d'un patient.
- Enfin, un infirmier travaille dans l'hôpital. Il n'est pas affecté à un service particulier et ce n'est pas un médecin. Il peut lire et créer le dossier d'un patient. En revanche, il ne peut pas modifier le dossier d'un patient.
< à personne

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.

Quels sont les rôles hiérarchiquement inférieurs à Médecin ?

- | | |
|--|---|
| <input checked="" type="checkbox"/> a. Radiologue | ✖ |
| <input checked="" type="checkbox"/> b. Pédiatre | ✖ |
| <input checked="" type="checkbox"/> c. Ophtalmologue | ✖ |
| <input type="checkbox"/> d. Stagiaire_radiologue | |
| <input type="checkbox"/> e. Stagiaire_pédiatre | |
| <input type="checkbox"/> f. Stagiaire_ophtalmologue | |
| <input type="checkbox"/> g. Infirmier | |
| <input type="checkbox"/> h. Aucun | |

Votre réponse est incorrecte.

La hiérarchie est la suivante :

Médecin < Radiologue

Médecin < Pédiatre

Médecin < Ophtalmologue

Stagiaire_radiologue < Radiologue

Stagiaire_pédiatre < Pédiatre

Stagiaire_ophtalmologue < Ophtalmologue

C'est tout !

La réponse correcte est :

Aucun

Question 25

Partiellement correct

Note de 0,50 sur 1,00

Autorisation question 2

Quels sont les rôles hiérarchiquement inférieurs à Radiologue ?

- a. Médecin
- b. Pédiatre
- c. Ophtalmologue
- d. Stagiaire_radiologue
- e. Stagiaire_pédiatre
- f. Stagiaire_ophtalmologue
- g. Infirmier
- h. Aucun



Votre réponse est partiellement correcte.

Vous en avez sélectionné correctement 1.

Les réponses correctes sont :

Médecin,

Stagiaire_radiologue

Question 26

Correct

Note de 1,00 sur 1,00

Autorisation question 3**Quels sont les rôles hiérarchiquement inférieurs à Stagiaire_pédiatre ?**

- a. Médecin
- b. Radiologue
- c. Pédiatre
- d. Ophtalmologue
- e. Stagiaire_radiologue
- f. Stagiaire_ophtalmologue
- g. Infirmier
- h. Aucun

**Votre réponse est correcte.****La réponse correcte est :**

Aucun

Question 27

Correct

Note de 1,00 sur 1,00

Autorisation question 4**Quels sont les rôles hiérarchiquement inférieurs à Infirmier ?**

- a. Médecin
- b. Radiologue
- c. Pédiatre
- d. Ophtalmologue
- e. Stagiaire_radiologue
- f. Stagiaire_pédiatre
- g. Stagiaire_ophtalmologue
- h. Aucun

**Votre réponse est correcte.****La réponse correcte est :**

Aucun

Question 28

Correct

Note de 1,00 sur 1,00

Autorisation question 5

Le couple <a, g> représente la permission de réaliser l'action a sur une ressource du groupe local g.

Par exemple <lire, dossier_patient_radiologie> représente la permission de lire les ressources du groupe dossier_patient_radiologie.

Quelles sont les permissions affectées au rôle médecin ?

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

- a. <créer, dossier_patient_radiologie>
- b. <lire, dossier_patient_radiologie> ✓
- c. <modifier, dossier_patient_radiologie>
- d. <créer, dossier_patient_pédiatrie>
- e. <lire, dossier_patient_pédiatrie > ✓
- f. <modifier, dossier_patient_pédiatrie >
- g. <créer, dossier_patient_ophtalmologie>
- h. <lire, dossier_patient_ophtalmologie > ✓
- i. <modifier, dossier_patient_ophtalmologie >

Votre réponse est correcte.

Les réponses correctes sont :

<lire, dossier_patient_radiologie>,
<lire, dossier_patient_pédiatrie >,
<lire, dossier_patient_ophtalmologie >

Question 29

Correct

Note de 1,00 sur 1,00

Autorisation question 6**Quelles sont les permissions affectées au rôle radiologue ?****Important : ne pas affecter une permission à un rôle si ce rôle hérite déjà de cette permission d'un rôle hiérarchiquement inférieur.**

- a. <créer, dossier_patient_radiologie> ✓
- b. <lire, dossier_patient_radiologie>
- c. <modifier, dossier_patient_radiologie> ✓
- d. <créer, dossier_patient_pédiatrie>
- e. <lire, dossier_patient_pédiatrie >
- f. <modifier, dossier_patient_pédiatrie >
- g. <créer, dossier_patient_ophtalmologie>
- h. <lire, dossier_patient_ophtalmologie >
- i. <modifier, dossier_patient_ophtalmologie >

Votre réponse est correcte.**Les réponses correctes sont :**

<créer, dossier_patient_radiologie>,
<modifier, dossier_patient_radiologie>

Question 30

Correct

Note de 1,00 sur 1,00

Autorisation question 7**Quelles sont les permissions affectées au rôle stagiaire_pédiatre ?****Important : ne pas affecter une permission à un rôle si ce rôle hérite déjà de cette permission d'un rôle hiérarchiquement inférieur.**

- a. <créer, dossier_patient_radiologie>
- b. <lire, dossier_patient_radiologie>
- c. <modifier, dossier_patient_radiologie>
- d. <créer, dossier_patient_pédiatrie> ✓
- e. <lire, dossier_patient_pédiatrie > ✓
- f. <modifier, dossier_patient_pédiatrie >
- g. <créer, dossier_patient_ophtalmologie>
- h. <lire, dossier_patient_ophtalmologie >
- i. <modifier, dossier_patient_ophtalmologie >

Votre réponse est correcte.**Les réponses correctes sont :**

<créer, dossier_patient_pédiatrie>,

<lire, dossier_patient_pédiatrie >

Question 31

Correct

Note de 1,00 sur 1,00

Autorisation question 8**Quelles sont les permissions affectées au rôle infirmier ?****Important : ne pas affecter une permission à un rôle si ce rôle hérite déjà de cette permission d'un rôle hiérarchiquement inférieur.**

- | | |
|---|---|
| <input checked="" type="checkbox"/> a. <créer, dossier_patient_radiologie> | ✓ |
| <input checked="" type="checkbox"/> b. <lire, dossier_patient_radiologie> | ✓ |
| <input type="checkbox"/> c. <modifier, dossier_patient_radiologie> | |
| <input checked="" type="checkbox"/> d. <créer, dossier_patient_pédiatrie> | ✓ |
| <input checked="" type="checkbox"/> e. <lire, dossier_patient_pédiatrie > | ✓ |
| <input type="checkbox"/> f. <modifier, dossier_patient_pédiatrie > | |
| <input checked="" type="checkbox"/> g. <créer, dossier_patient_ophtalmologie> | ✓ |
| <input checked="" type="checkbox"/> h. <lire, dossier_patient_ophtalmologie > | ✓ |
| <input type="checkbox"/> i. <modifier, dossier_patient_ophtalmologie > | |

Votre réponse est correcte.**Les réponses correctes sont :**

<créer, dossier_patient_radiologie>,
<lire, dossier_patient_radiologie>,
<créer, dossier_patient_pédiatrie>,
<lire, dossier_patient_pédiatrie >,
<créer, dossier_patient_ophtalmologie>,
<lire, dossier_patient_ophtalmologie >

Question 32

Incorrect

Note de 0,00 sur 1,00

Autorisation Question 9

L'hôpital souhaite ajouter la contrainte suivante : un médecin ne peut cumuler les rôles de radiologue et pédiatre.

Comment proposeriez-vous de prendre en compte cette contrainte ?

- a. **Une contrainte de séparation des pouvoirs statique (SSOD) entre les rôles radiologue et pédiatre**
- b. Une contrainte de cardinalité sur le nombre de rôles qui peut être affecté au médecin
- c. Une contrainte de séparation des pouvoirs dynamique (DSOD) entre les rôles radiologue et pédiatre ✗
- d. 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

Votre réponse est incorrecte.

La réponse correcte est :

Une contrainte de séparation des pouvoirs statique (SSOD) entre les rôles radiologue et pédiatre

Question 33

Incorrect

Note de 0,00 sur 1,00

Autorisation Question 10

L'hôpital souhaite ajouter la contrainte suivante : un stagiaire ne peut activer en même temps les rôles de stagiaire_radiologue et stagiaire_pédiatre.

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 statique (SSOD) entre les rôles stagiaire_radiologue et stagiaire_pédiatre
- c. **Une contrainte de séparation des pouvoirs dynamique (DSOD) entre les rôles stagiaire_radiologue et stagiaire_pédiatre**
- d. Il n'y a pas besoin d'ajouter de contrainte : le stagiaire hérite de la contrainte qui empêche un médecin de cumuler les rôles de radiologue et pédiatre.

Votre réponse est incorrecte.

La réponse correcte est :

Une contrainte de séparation des pouvoirs dynamique (DSOD) entre les rôles stagiaire_radiologue et stagiaire_pédiatre

Question 34

Incorrect

Note de 0,00 sur 1,00

Autorisation Question 11

L'hôpital souhaite ajouter la contrainte suivante : un médecin ne devrait pas cumuler les permissions de modifier les dossiers du groupe dossier_patient_radiologie et du groupe dossier_patient_ophtalmologie.

Comment proposeriez-vous de prendre en compte cette contrainte ?

- a. Une contrainte de cardinalité sur le nombre de permissions qui peut être affecté au médecin
- b. **On ne peut pas directement exprimer cette contrainte dans le modèle AGLP. La meilleure solution est d'introduire une contrainte de séparation des pouvoirs statique (SSOD) entre les rôles radiologue et ophtalmologue**
- c. On ne peut pas directement exprimer cette contrainte dans le modèle AGLP. La meilleure solution est d'introduire une contrainte de séparation des pouvoirs dynamique (SSOD) entre les rôles radiologue et ophtalmologue
- d. Deux possibilités : (1) Il faut enlever, au rôle radiologue, la permission de modifier les dossiers du groupe dossier_patient_radiologie ou alors (2) il faut enlever, au rôle ophtalmologue, la permission de modifier les dossiers du groupe dossier_patient_ophtalmologie

Votre réponse est incorrecte.

La réponse correcte est :

On ne peut pas directement exprimer cette contrainte dans le modèle AGLP. La meilleure solution est d'introduire une contrainte de séparation des pouvoirs statique (SSOD) entre les rôles radiologue et ophtalmologue

Question 35

Correct

Note de 1,00 sur 1,00

Contrôle d'accès obligatoire (MAC)

Laquelle de ces propriétés de sécurité ou caractéristiques ne fait pas partie du modèle de Bell et La Padula sous-jacent au contrôle d'accès obligatoire (Mandatory Access Control ou MAC)

- a. **Séparation des pouvoirs (Separation of Duty)** ✓
- b. Étiquette de classification des données et étiquette d'habilitation des utilisateurs
- c. No Read Up
- d. No Write Down

Votre réponse est correcte.

La réponse correcte est : Séparation des pouvoirs (Separation of Duty)

Question 36

Correct

Note de 1,00 sur 1,00

Authentification - quelque chose qu'on possède

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

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

Votre réponse est correcte.

La réponse correcte est :

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

Question 37

Correct

Note de 1,00 sur 1,00

Réseau privé virtuel (VPN)

Par rapport aux caractéristiques et fonctionnalités d'un réseau privé virtuel (VPN) utilisant le protocole IPSEC en mode tunnel, laquelle de ces réponses est fausse :

- a. Ce mode est incompatible avec l'utilisation d'un routeur NAT et des sous-réseaux avec adresses privées (10.X.Y.Z, 192.168.X.Y, etc.) ✓
- b. Ce mode permet de chiffrer le trafic IP entre deux correspondants à travers l'Internet
- c. Ce mode permet d'assurer l'intégrité des paquets IP transmis entre correspondants du même réseau virtuel
- d. Ce mode établit un concept de "session" permettant d'éviter la transmission des paramètres cryptographiques à chaque paquet

Votre réponse est correcte.

La réponse correcte est :

Ce mode est incompatible avec l'utilisation d'un routeur NAT et des sous-réseaux avec adresses privées (10.X.Y.Z, 192.168.X.Y, etc.)

Question 38

Incorrect

Note de 0,00 sur 1,00

Révocation de certificats

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

- a. 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. ✓
- b. L'autorité de certification peut décider de révoquer un certificat. L'autorité de certification doit supprimer le certificat lorsqu'il a été révoqué. ✗
- c. 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. ✓
- d. Chaque certificat possède une date d'expiration. L'autorité de certification doit supprimer le certificat lorsque la date d'expiration est atteinte. ✗

Votre réponse est incorrecte.

Les réponses correctes sont :

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.,

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.

[◀ Annonces](#)[Aller à...](#)

Commencé le vendredi 30 avril 2021, 09:30

État Terminé

Terminé le vendredi 30 avril 2021, 11:29

Temps mis 1 heure 59 min

Points 32,00/39,00

Note 32,82 sur 40,00 (82%)

Question 1

Correct

Note de 1,00 sur 1,00

Dans le modèle "standard" d'une attaque via le réseau, la phase de reconnaissance consiste à :

- a. Identifier les caractéristiques techniques de la cible (configuration, logiciels installés, etc.)
- b. Reconnaître si la cible trouvée est d'intérêt pour l'attaquant
- c. Extraire vers l'extérieur le plus d'information possible des bases de données et fichiers contenu sur la cible
- d. Repérer "où" sur le réseau se trouve la ou les cibles des attaques, p.ex. nom de domaine, adresse IP



La réponse correcte est :

Repérer "où" sur le réseau se trouve la ou les cibles des attaques, p.ex. nom de domaine, adresse IP

Question 2

Incorrect

Note de 0,00 sur 1,00

Laquelle de ces réponses n'est pas une caractéristique de la détection par règle :

- a. La détection par règle à le désavantage que si l'attaquant connaît la règle de détection il peut souvent trouver une façon de réaliser son activité de piratage sans déclencher cette règle
- b. Il n'est pas nécessaire qu'un humain examine les alertes d'un IDS par règle, car celle-ci sont facilement interprétable par un algorithme automatique de protection des systèmes.
- c. La détection par règle n'a pas de période d'"apprentissage" des activités normales du réseau et peut-être déployée immédiatement
- d. Il existe un compromis entre taux de faux positif (fausse alertes) et taux de faux négatif (alertes manquées), souvent déterminé par le seuil de détection

✗

La réponse correcte est :

Il n'est pas nécessaire qu'un humain examine les alertes d'un IDS par règle, car celle-ci sont facilement interprétable par un algorithme automatique de protection des systèmes.

Question 3

Correct

Note de 1,00 sur 1,00

Laquelle de ces réponses n'est pas un type d'attaque de déni de service :

- a. Attaque de déni de service distribuée (Distributed DoS)
- b. Attaque par exploitation d'une porte dérobée (Backdoor DoS)
- c. Attaque par inondation HTTP (HTTP Flooding)
- d. Attaque par vulnérabilité (Crippling DoS)

✓

La réponse correcte est :

Attaque par exploitation d'une porte dérobée (Backdoor DoS)

Unlike other DoS attacks that aim to flood a system with traffic, crippling DoS attacks are more strategic and focus on exploiting specific vulnerabilities in the target system. These attacks can take various forms, such as flooding a target with bogus packets, exploiting vulnerabilities in the application or network stack, or simply overwhelming the target with a huge number of legitimate requests. Crippling DoS attacks can be launched from a single source or from a distributed network of computers or botnets.

Question 4

Incorrect

Note de 0,00 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 informatiques sur des applications Web pour toutes ces raisons sauf

- a. La requête SQL est précompilée par le moteur de base de données ce qui permet qu'elle soit exécutée plus rapidement qu'une requête SQL transmise par le réseau, qui elle est interprétée et exécutée en temps réel
- b. L'utilisation de stored procedures permet de restreindre l'utilisation de SQL à seulement les requêtes qui sont nécessaires pour la bonne exécution de l'application Web
- c. Des permissions peuvent être attribuées à niveau de la stored procedure correspondant à des groupes d'utilisateurs restreints
- d. Parce que le code SQL des stored procedure est pré-déterminé d'avance, du code SQL contenu dans des chaînes de caractère passées en paramètres au stored procedure ne serait pas interprété comme du code SQL, juste comme une chaîne de caractère.

vitesse de compilation aucun rapport avec sécurité

La réponse correcte est :

La requête SQL est précompilée par le moteur de base de données ce qui permet qu'elle soit exécutée plus rapidement qu'une requête SQL transmise par le réseau, qui elle est interprétée et exécutée en temps réel

Question 5

Correct

Note de 1,00 sur 1,00

Par rapport aux caractéristiques et fonctionnalités d'un réseau privé virtuel (VPN) utilisant le protocole IPSEC, laquelle de ces réponses est fausse :

- a. Établit un concept de "session" permettant d'éviter la transmission des paramètres cryptographiques à chaque paquet
- b. Permet de chiffrer le trafic IP entre deux correspondants à travers l'Internet
- c. Permet d'assurer l'intégrité des paquets IP transmis entre correspondants du même réseau virtuel
- d. Est incompatible avec l'utilisation d'un routeur NAT et des sous-réseaux avec adresses privées (10.X.Y.Z, 192.168.X.Y, etc.)

La réponse correcte est :

Est incompatible avec l'utilisation d'un routeur NAT et des sous-réseaux avec adresses privées (10.X.Y.Z, 192.168.X.Y, etc.)

SSL/TLS établit une session avant la transmission
des données

IPsec mode tunnel compatible avec NAT

Question 6

Incorrect

Note de 0,00 sur 1,00

Laquelle des réponses suivantes n'est pas une contre-mesure efficace contre les attaques par débordement de tampon sur la pile.

- a. Utiliser des langages de programmation plus modernes tel que le Javascript
- b. Configurer le système d'exploitation pour que l'espace mémoire alloué soit attribué aléatoirement (ASLR)
- c. Programmer de façon à éviter de passer des pointeurs de tampon en paramètre sans passer aussi l'information de la quantité de mémoire qui y a été allouée
- d. Déployer une solution de protection des pointeurs de retour du type canari (tel que Stack Guard)

La réponse correcte est :

Utiliser des langages de programmation plus modernes tel que le Javascript

Question 7

Correct

Note de 1,00 sur 1,00

La sécurité des protocoles SSL et TLS repose sur la fiabilité de l'infrastructure à clé publique (ICP) déployée pour assurer l'authenticité des certificats de clé publique envoyé par les serveurs Web lors de l'établissement d'une connexion SSL/TLS. Un des problèmes de cette ICP est le fait qu'elle est hiérarchique et qu'elle repose sur la fiabilité des plusieurs autorité de certification racine (root CA) présentement supportés par l'ensemble des fureteurs Web présentement utilisés par la majorité des usagers. Laquelle de ces réponses n'est pas une raison (ou est la raison la plus faible) pour mettre en doute la fiabilité de ces autorités racine et donc questionner la sécurité de SSL/TLS.

- a. Certaines autorités racines signent les certificats avec des algorithmes de clé publique qui ne sont même pas résistants à des attaques de cryptanalyse quantique
- b. Le processus de vérification de l'identité des personnes et de la propriété d'un domaine par la personne ou organisation qui demande un certificat n'est pas standard et varie d'une autorité racine à l'autre
- c. Il y a très peu d'informations disponibles sur certaines de ces autorités racines, ce qui rend difficile de vérifier quels sont les intérêts (commerciaux ou autres) qui sont derrière ces autorités racines.
- d. Certaines des autorités racines sont de petites organisations à but non lucratif qui pourraient être vulnérables à des attaques informatiques ciblées dont le but serait de voler les clés privées utilisées pour la signature de certificat.

La réponse correcte est :

Certaines autorités racines signent les certificats avec des algorithmes de clé publique qui ne sont même pas résistants à des attaques de cryptanalyse quantique

Question 8

Correct

Note de 1,00 sur 1,00

Concernant les attaques de Cross-Site Scripting (XSS) contre des serveurs Web, laquelle de ces affirmations est vraie:

- a. Elles permettent de prendre le contrôle ("owner") du serveur Web qui démontre ce type de vulnérabilité
- b. Elle permet de relayer le client (fureteur) sur un site malveillant avec les mêmes priviléges que s'il était sur le site qui a la vulnérabilité ✓
- c. Ne sont pas possibles si le site ciblé utilise le protocole SSL ou TLS pour protéger la session HTTP
- d. Sont en général possibles grâce à la présence d'une vulnérabilité de type débordement de tampon sur le tas dans l'application Web

La réponse correcte est :

Elle permet de relayer le client (fureteur) sur un site malveillant avec les mêmes priviléges que s'il était sur le site qui a la vulnérabilité

Question 9

Correct

Note de 1,00 sur 1,00

Laquelle des raisons mentionnées n'est pas une bonne réponse en ce qui concerne la difficulté de créer du "shell code" qui puisse être utilisé dans une attaque par débordement de tampon sur une application vulnérable :

- a. L'utilisation de NOP sled (chaîne de plusieurs 0x90) est problématique car elle peut facilement être détectée par un IDS ou autre produit de sécurité
- b. Le shell code doit rester suffisamment petit afin de pouvoir rentrer dans son entiereté dans le buffer et l'espace entre celui ci et le pointeur de retour
- c. La distance entre le début du tampon et le pointeur de retour n'est pas toujours la même car l'exécution du programme n'est pas déterministe
- d. Il faut absolument éviter que le shell code contiennent des caractères NULL (0x00) qui pourraient facilement être détectés par des IDS ou autre type d'outils de sécurité informatique ✓

La réponse correcte est :

Il faut absolument éviter que le shell code contiennent des caractères NULL (0x00) qui pourraient facilement être détectés par des IDS ou autre type d'outils de sécurité informatique

Question 10

Correct

Note de 1,00 sur 1,00

Lequel de ce type de vulnérabilité logiciel ne peut pas être adresser en utilisant des techniques vérification et validation des entrées d'un programme

- a. Débordement de tampon sur la pile
- b. SQL Injection
- c. Cross-site Scripting (XSS)
- d. Erreur de logique d'application



La réponse correcte est :

Erreur de logique d'application

Question 11

Correct

Note de 1,00 sur 1,00

Concernant l'utilisation des secure token dans les applications Web, laquelle de ces affirmations est fausse

- a. L'utilisation de secure token est un moyen de protection contre le Cross Site Request Forgery (XSRF)
- b. Un "secure token" est la même chose qu'un "session ID"
- c. La valeur d'un secure token est choisie et vérifiée par le serveur en correspondance avec le session ID
- d. Sur le fureteur du client, le secure token est éphémère et n'est pas stocké dans la base de données de cookies



La réponse correcte est :

Un "secure token" est la même chose qu'un "session ID"

Question 12

Correct

Note de 1,00 sur 1,00

Laquelle de ces réponses ne constitue pas une attaque rendue possible par une vulnérabilité logiciel :

- a. Attaque cryptanalytique utilisant une faiblesse d'un l'algorithme de chiffrement obsolète utilisé dans le logiciel ✓
- b. Vulnérabilité de la chaîne de format (format string vulnerability)
- c. Attaque de déni de service de type "crippling DoS"
- d. Débordement de tampon sur le tas (heap buffer overflow)

n'est pas une faiblesse dans le code personnel du programmeur ?

La réponse correcte est :

Attaque cryptanalytique utilisant une faiblesse d'un l'algorithme de chiffrement obsolète utilisé dans le logiciel

Question 13

Correct

Note de 1,00 sur 1,00

Le contrôle d'accès aux biens informatiques inclut les aspects suivants sauf

- a. Identification ("Identification")
- b. Autorisation ("Authorization")
- c. Disponibilité ("Availability") ✓
- d. Authentification ("Authentication")

La réponse correcte est :

Disponibilité ("Availability")

Question 14

Correct

Note de 1,00 sur 1,00

Laquelle de ces informations est fausse par rapport au contrôle d'accès discrétionnaire (Discretionary Access Control ou DAC)

- a. Les usagers peuvent changer les permissions des fichiers qui leur appartiennent
- b. Est plus permissif que le modèle de contrôle d'accès obligatoire (Mandatory Access Control ou MAC)
- c. C'est le modèle de contrôle d'accès utilisé pour les fichiers par les systèmes d'exploitation Linux et Windows
- d. Implémente la règle "no write down" qui empêche un programme d'écrire dans un fichier pour lesquels il n'a pas le bon niveau d'accès ✓

La réponse correcte est :

Implémente la règle "no write down" qui empêche un programme d'écrire dans un fichier pour lesquels il n'a pas le bon niveau d'accès

Question 15

Correct

Note de 1,00 sur 1,00

Laquelle de ces propriétés de sécurité ou caractéristiques ne fait pas partie du modèle Bell et La Padula sous-jacent au contrôle d'accès obligatoire (Mandatory Access Control ou MAC)

- a. No Write Down
- b. Étiquetage des données en fonction de leur niveau de confidentialité ("classification")
- c. Domain Type Enforcement (DTE) ✓
- d. No Read Up

La réponse correcte est :

Domain Type Enforcement (DTE)

Question 16

Correct

Note de 1,00 sur 1,00

Laquelle de ces informations sur le contrôle d'accès basé sur les rôles (Role-based Access Control ou RBAC) est fausse

- a. La philosophie AGLP (Access, Global, Local, Permissions) est un exemple d'application de la méthode RBAC
- b. Ce modèle essaie de minimiser la complexité de la gestion des accès des usagers individuels
- c. Un sujet ne peut pas jouer plusieurs rôles dans la même session
- d. Le modèle RBAC associe les droits d'accès à une notion de session car le même usager ne joue pas toujours le même rôle

sujet peut jouer plusieurs roles dans la meme session

La réponse correcte est :

Un sujet ne peut pas jouer plusieurs rôles dans la même session

Question 17

Correct

Note de 1,00 sur 1,00

La contrainte RBAC qui empêche que le même usager puisse remplir deux rôles précis dans la même session s'appelle:

- a. Single Role Access Control Policy
- b. Une telle contrainte n'existe pas dans RBAC: un utilisateur peut toujours remplir deux rôles ou plus dans la même session
- c. No write down
- d. Separation of Duty

différents travaux ne peuvent pas être
performé par la même personne de la session

La réponse correcte est :

Separation of Duty

Question 18

Correct

Note de 1,00 sur 1,00

Laquelle des réponses suivantes n'est pas une propriété ou objectif de la signature numérique

- a. Authenticité du message
- b. Non répudiation
- c. Confidentialité du message
- d. Intégrité du message



La réponse correcte est :

Confidentialité du message

Question 19

Correct

Note de 1,00 sur 1,00

Laquelle de ces réponses n'est pas un objectif ou un principe de la gestion des identités et des accès (GIA, ou Identity Access Management - IAM en anglais)

- a. La séparation entre les fonctions de contrôle d'accès (authentification et autorisation) et les fonctions du système (logique d'application, règles d'affaires, etc.)
- b. Assurer une gestion intégrée et centraliser des paramètres d'authentification et des permissions d'accès
- c. Provisionnement de solution intégrée d'authentification avec l'utilisation de solution de Single Sign On (SSO)
- d. La comparaison continue entre les accès attribués dans le système d'IAM et les politiques de sécurité



La réponse correcte est :

Provisionnement de solution intégrée d'authentification avec l'utilisation de solution de Single Sign On (SSO)

Question 20

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 de métal utilisé 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'usager, qui est envoyé à un serveur par Internet ✓ pour authentifier l'usager
- d. Un téléphone portable intelligent utilisé pour générer un mot de passe à usage unique

quelque chose que je suis

La réponse correcte est :

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

Question 21

Correct

Note de 1,00 sur 1,00

Un des principaux avantages de l'utilisation de la cryptographie à courbe elliptique (Elliptic Curve Cryptography ou ECC) est

- a. qu'elle est plus résistante aux attaques de cryptanalyse post-quantique
- b. que son utilisation est gratuite car elle ne repose pas sur des brevets commerciaux
- c. qu'elle peut être rendue très performante grâce à l'utilisation de GPU pour calculer les points sur des courbes elliptiques en 3D
- d. est le fait que pour un niveau de sécurité équivalent la taille des clés est plus petite, ce qui rend les signatures plus petites également, ce qui est attractif dans des applications où la bande passante est réduite ✓

La réponse correcte est :

est le fait que pour un niveau de sécurité équivalent la taille des clés est plus petite, ce qui rend les signatures plus petites également, ce qui est attractif dans des applications où la bande passante est réduite

Question 22

Correct

Note de 1,00 sur 1,00

Laquelle de ces affirmation sur l'utilisation de solutions de gestion centralisé de mots de passe (Singe Sign On ou SSO) est fausse

- a. A comme désavantage de constituer un point de défaillance unique
- b. La base de données de mots de passe doit être protéger par un mot de passe "maître" qui les protège tous
- c. Protège contre les compromissions de données d'authentification (p.ex. /etc/shadow) dans les serveurs d'authentification ✓
- d. Elle a l'avantage de permettre à l'utilisateur de choisir des mots de passe de plus haute entropie

La réponse correcte est :

Protège contre les compromissions de données d'authentification (p.ex. /etc/shadow) dans les serveurs d'authentification

Question 23

Correct

Note de 1,00 sur 1,00

Malgré que plusieurs experts (y compris le président Obama) aient annoncée la mort imminente du mot de passe, les nouvelles de sa mort semble avoir été grandement exagérée. Laquelle de ces raisons n'est pas une des raisons de son succès passé et présent.

- a. Son utilisation ne nécessite daucun matériel (hardware) supplémentaire et a donc un coût supplémentaire négligeable
- b. Si le mot de passe d'un usager est compromis, il est relativement facile pour celui-ci de le ré-initialiser, ce qui permet de réduire l'impact d'une telle situation
- c. C'est un des rares facteurs d'authentification qui puisse être utilisé facilement à travers un réseau informatique
- d. L'authentification par mot de passe n'est pas vulnérable aux attaques de rejeu ✓

La réponse correcte est :

L'authentification par mot de passe n'est pas vulnérable aux attaques de rejeu

Question 24

Incorrect

Note de 0,00 sur 1,00

Par rapport à la cryptographie post-quantique laquelle de ces affirmations est vraie

- a. La plupart des algorithmes de cryptographie post-quantique ont une performance similaire à celle des algorithmes cryptographiques équivalents actuels
- b. Ce terme désigne les algorithmes de cryptographie à clé symétrique pour lesquels aucun algorithme de cryptanalyse quantique efficace est connu
- c. Il existe déjà plusieurs algorithmes de cryptographie post-quantique qui ont été sélectionnés et évalués par des institutions de normes et standardisation
- d. Constitue une préoccupation essentiellement "académique" et peu urgente car aucun ordinateur quantique suffisamment grand ✕ n'a été construit pour implémenter les algorithmes de cryptanalyse quantique

La réponse correcte est :

Il existe déjà plusieurs algorithmes de cryptographie post-quantique qui ont été sélectionnés et évalués par des institutions de normes et standardisation

Question 25

Terminer

Non noté

Laquelle de ces affirmations sur l'authentification par défi-réponse (Challenge-response) est vraie

- a. N'est utilisé que pour des applications Web
- b. Ne nécessite pas que le défi (challenge) soit choisi avec une haute entropie
- c. Ne permet pas que le serveur Bob puisse authentifier le client Alice
- d. Ne protège pas contre les attaques par rejet

La réponse correcte est :

Ne permet pas que le serveur Bob puisse authentifier le client Alice

Question 26

Correct

Note de 1,00 sur 1,00

L'entropie fait partie de la réponse à toutes ces questions sauf

- a. La difficulté de factoriser des grands entiers afin de retrouver des clés privées dans certains algorithmes à clé publique ✓
- b. La difficulté de conduire une attaque par force brute sur un système d'authentification par mot de passe
- c. L'utilisation adéquate d'un codage en terme résistance à des efforts cryptanalytiques par texte clair choisi
- d. L'efficacité des algorithmes de compression

La réponse correcte est :

La difficulté de factoriser des grands entiers afin de retrouver des clés privées dans certains algorithmes à clé publique

Question 27

Correct

Note de 1,00 sur 1,00

Laquelle de ces méthodes n'est pas adéquate pour assurer l'authenticité d'un message envoyé par Alice à Bob dans un contexte où Ève peut intercepter et modifier le message envoyé d'Alice à Bob de façon imperceptible.

- a. Utilisation de signature numérique par Alice pour signer le message avant de le transmettre à Bob avec le certificat de clé publique d'Alice
- b. Utiliser une fonction de hachage pour calculer le haché du message qui est transmis par Alice à Bob en utilisant un canal alternatif
- c. Utiliser le protocole HMAC en s'assurant qu'Alice et Bob aient préalablement échanger un secret partagé S
- d. Utilisation du protocole d'échange de clés de Diffie-Hellman pour échanger une clé secrète qui peut être utiliser pour le protocole HMAC ✓

c'est une des étapes pas tout

La réponse correcte est :

Utilisation du protocole d'échange de clés de Diffie-Hellman pour échanger une clé secrète qui peut être utiliser pour le protocole HMAC

Question 28

Correct

Note de 1,00 sur 1,00

Laquelle de ces affirmations est vraie concernant la cryptographie quantique

- a. Est une construction théorique pour laquelle aucune démonstration expérimentale ni solution disponible commercialement existe
- b. Ce terme désigne les algorithmes de cryptographie qui sont résistants aux attaques de cryptanalyse quantique
- c. A été récemment découverte par des chercheurs en Chine
- d. Ce terme désigne des algorithmes de cryptographie qui se basent sur les propriétés de la physique quantique pour assurer leur sécurité ✓

La réponse correcte est :

Ce terme désigne des algorithmes de cryptographie qui se basent sur les propriétés de la physique quantique pour assurer leur sécurité

Question 29

Correct

Note de 1,00 sur 1,00

Plusieurs annoncent depuis plusieurs années la mort imminente du mot de passe comme mécanisme d'authentification sur les systèmes informatiques (y compris même le président américain Barak Obama!). Laquelle de ces caractéristiques constitue la raison principale pour laquelle le mot de passe est "mort".

- a. La sécurité de l'authentification par mot de passe peut être compromise par la capture des bases de données de hachés de mots de passe
- b. L'authentification par mot de passe est vulnérable à des attaques par logiciel malveillant tel que des enregistreurs de touches (keylogger)
- c. Aujourd'hui, les mots de passe utilisés pour l'authentification dans les applications Web peuvent facilement être capturés par une Ève qui peut intercepter les paquets IP transmis entre le fureteur d'Alice et le serveur Web de Bob.
- d. Il est peu naturel (et donc peu fréquent) pour les usagers de choisir des mots de passe avec haute entropie et qui soient en même temps facile à retenir ✓

La réponse correcte est :

Il est peu naturel (et donc peu fréquent) pour les usagers de choisir des mots de passe avec haute entropie et qui soient en même temps facile à retenir

Question 30

Correct

Note de 1,00 sur 1,00

En cryptographie le principe de souveraineté de clé (choisissez la bonne réponse)

- a. Dit que les clés cryptographiques devraient être générées par la personne ou l'autorité à qui cette clé appartient et qui va l'utiliser ✓
- b. Qu'un état souverain devrait avoir la capacité d'intercepter des communications protégées par une clé cryptographique s'il a une raison légitime pour le faire (p.ex. mandat judiciaire d'écoute, sécurité nationale, etc.)
- c. Consiste à s'assurer qu'une clé cryptographique symétrique ne puisse être partagée que par des individus ayant le même niveau d'accès, et en particulier citoyen d'un même pays
- d. Implique qu'une clé cryptographique ne devrait servir qu'à un seul usage (p.ex. signer ou chiffrer, mais pas les deux)

La réponse correcte est :

Dit que les clés cryptographiques devraient être générées par la personne ou l'autorité à qui cette clé appartient et qui va l'utiliser

Question 31

Correct

Note de 1,00 sur 1,00

Laquelle de ces informations est fausse concernant l'algorithme cryptographique du masque jetable

- a. Permet une sécurité parfaite en autant que la taille de la clé soit aussi grande que celle du message et qu'elle soit choisie avec une entropie maximale
- b. Est résistant à la cryptanalyse quantique
- c. N'est pas performant car elle demande des temps de calcul considérablea, même pour des fichiers de taille moyenne (quelques MB)
- d. Aurait été utilisé par le Che Guevara pour transmettre ou recevoir des informations chiffrées envoyées à La Havane lorsqu'il menait des opérations de guerrilla en Bolivie peu avant sa mort.

Les réponses correctes sont :

Permet une sécurité parfaite en autant que la taille de la clé soit aussi grande que celle du message et qu'elle soit choisie avec une entropie maximale,

N'est pas performant car elle demande des temps de calcul considérablea, même pour des fichiers de taille moyenne (quelques MB)

Question 32

Correct

Note de 1,00 sur 1,00

Qu'est-ce qui est vrai concernant l'utilisation de techniques de correction d'erreur ?

- a. La correction d'erreur à partir du syndrome doit être fait avant le déchiffrement du message ✓
- b. Elle permet de protéger l'intégrité du contenu du message contre un attaquant malveillant
- c. Le calcul et l'ajout du syndrome doit être fait le plus tôt possible, soit à la couche la plus haute du modèle ISO (idéalement couche application)
- d. Son lien avec l'entropie du message est décrit par le 1er théorème de Shannon

La réponse correcte est :

La correction d'erreur à partir du syndrome doit être fait avant le déchiffrement du message

Question 33

Terminer

Note de 2,00 sur 2,00

Qu'est-ce qui est vrai concernant l'utilisation de techniques de correction d'erreur ?

Expliquez votre choix de réponse à la question antérieure.

Le lien avec l'entropie du message est décrit par le 2ième théorème de Shannon. Le chiffrement et déchiffrement ne corrige pas les erreurs et il faut donc appliquer le syndrome après le chiffrement et avant le déchiffrement puisqu'une erreur introduite entre le chiffrement et le déchiffrement pourrait donner un tout autre message considérant la propriété de diffusion recherché par les algorithmes de chiffrement.

Question 34

Correct

Note de 1,00 sur 1,00

Lequel de ces services doit absolument être placé dans la DMZ

- a. Serveur de base de données utilisée par une application Web externe
- b. **Proxy web applicatif protégeant les connexions sortantes** ✓
- c. Serveur mail IMAP et POP3 permettant aux usagers d'accéder à leurs boîtes au lettre
- d. Serveur Web pour usager externe

Les réponses correctes sont :

Serveur Web pour usager externe,

Proxy web applicatif protégeant les connexions sortantes

Question 35

Terminer

Note de 2,00 sur 2,00

Lequel de ces services doit absolument être placé dans la DMZ

Explique votre réponse à la question précédente

Les serveurs mail ne seront définitivement pas dans la DMZ puisqu'ils sont pour usage interne.

Le serveur Web pour usager externe pourrait se retrouver dans la DMZ, mais l'utilisation d'un proxy web entre l'extérieur et le serveur web rend cela non-nécessaire.

Le serveur de base de données utilisée par une application Web externe communique aussi à travers le proxy web et ne sera donc pas dans la DMZ.

Au final, seul le proxy web doit être dans la DMZ puisque c'est celui-ci qui agit en tant que pont entre l'extérieur et l'intérieur rendant de la sorte tous les autres serveurs indirectement connecté à l'extérieur. Ils n'ont donc plus le besoin d'être dans la DMZ.

Question 36

Incorrect

Note de 0,00 sur 1,00

Laquelle de ces méthodes est la moins sécuritaire pour assurer l'authentification des usagers externes sur une application Web

- a. Faire la vérification du nom d'usager et mot de passe par du code client (sur le fureteur) écrit dans un langage sécuritaire comme le Java
- b. Stocker les noms d'usager et les mots de passe en clair dans le moteur de base de données utilisé par l'application Web, et faire la vérification du mot de passe à niveau du serveur Web
- c. Envoyer le nom d'usager et le mot de passe vers un serveur d'authentification externe qui fait la vérification
- d. Faire une vérification sur le serveur Web en utilisant le fichier /etc/passwd et/ou le fichier /etc/shadow sur ce serveur

La réponse correcte est : Faire la vérification du nom d'usager et mot de passe par du code client (sur le fureteur) écrit dans un langage sécuritaire comme le Java

Question 37

Terminer

Note de 0,00 sur 2,00

Laquelle de ces méthodes est la moins sécuritaire pour assurer l'authentification des usagers externes sur une application Web.

Expliquez votre réponse à la question précédente

L'envoi vers un serveur externe implique qu'il faut compromettre les deux serveurs et c'est donc plus difficile.

Dans le cas de la vérification sur le serveur, le mot de passe est haché nécessitant de déchiffrer celui-ci.

La vérification sur le fureteur peut impliquer certains dangers puisque l'utilisateur pourrait compromettre le code d'une certaine manière afin de permettre la connexion.

Cependant, le plus dangereux reste le stockage des noms d'usagers et mots de passe en clair puisqu'il suffit que le serveur web soit corrompu ou qu'il possède une faille logique afin qu'un attaquant récupère toutes les noms d'usagers et mots de passes des utilisateurs permettant ainsi d'avoir tous les accès.

◀ Annonces

Aller à...