

<b>Commencé le</b>	lundi 22 avril 2024, 14:00
<b>État</b>	Terminé
<b>Terminé le</b>	lundi 22 avril 2024, 14:51
<b>Temps mis</b>	51 min
<b>Points</b>	40,00/40,00
<b>Note</b>	<b>10,00</b> sur 10,00 (100%)

**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. Quand le programmeur écrit le programme
- ☐ b. Quand le programme est compilé
- ☒ c. Ce mécanisme est désormais natif dans la plupart des systèmes d'exploitation ✓
- ☐ d. Quand le programme est exécuté

Votre réponse est correcte.

La réponse correcte est :

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. Quand le programmeur écrit le programme
- ☒ b. Quand le programme est compilé ✓
- ☐ c. Ce mécanisme est désormais natif dans la plupart des systèmes d'exploitation
- ☐ d. Quand le programme est exécuté

Votre réponse est correcte.

La réponse correcte est :

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. 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
- ☐ b. 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
- ☐ 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 autre type 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 autre type d'outils de sécurité informatique

**Question 4**

Correct

Note de 2,00 sur 2,00

**Injection SQL**

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 (1=1 »

Requête mal formée



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 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 (1=1 » → Requête mal formée,

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 OR pwd = "blabla » → Authentification contournée

**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 ✓

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**

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 7**

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 ? (plusieurs réponses possibles)

- ☒ a. Vérifier que la requête ne contient pas de chaîne de caractères « -- » ✓
- ☒ b. Vérifier que la requête ne contient pas de chaîne de caractères « 1 = 1 » ✓
- ☐ 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 correspondant à une expression régulière de la forme « \d = \d » où \d est un chiffre ✓

Votre réponse est correcte.

Chiffrer le mot de 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 8**

Correct

Note de 2,00 sur 2,00

## 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 9**

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. 5
- ☐ b. 0,811
- ☒ c. 8,11 ✓
- ☐ d. 10

Votre réponse est correcte.

La réponse correcte est :  
8,11

**Question 10**

Correct

Note de 1,00 sur 1,00

## 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. 5
- ☐ b. 8,11
- ☐ c. 0,811
- ☒ d. 10 ✓

Votre réponse est correcte.

La réponse correcte est :  
10

**Question 11**

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.

Veuillez choisir une réponse.

- ☒ Vrai ✓
- ☐ Faux

La réponse correcte est « Vrai ».

**Question 12**

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 est de  $\frac{1}{3}$  et celle d'un 1 est de  $\frac{2}{3}$ .

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. 6,67
- ☐ b. 10
- ☐ c. 8,95
- ☒ d. 9,80 ✓

Votre réponse est correcte.

Probabilité d'apparition de 1 :  $\frac{1}{4} * \frac{2}{3} + \frac{3}{4} * \frac{1}{3} = \frac{2}{12} + \frac{3}{12} = \frac{5}{12}$

Probabilité d'apparition de 0 :  $\frac{1}{4} * \frac{1}{3} + \frac{3}{4} * \frac{2}{3} = \frac{1}{12} + \frac{6}{12} = \frac{7}{12}$

$E' = \frac{5}{12} * \log_2\left(\frac{12}{5}\right) + \frac{7}{12} * \log_2\left(\frac{12}{7}\right) = \frac{5}{12} * 1.26303 + \frac{7}{12} * 0.777608 = 0,98$

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

La réponse correcte est :

9,80



**Question 13**

Correct

Note de 1,00 sur 1,00

## Entropie Question 5

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

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

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

Votre réponse est correcte.

· Probabilité d'apparition de 0 :  $\frac{1}{4} * \frac{2}{3} + \frac{3}{4} * \frac{1}{3} + \frac{1}{4} * \frac{1}{3} = \frac{2}{12} + \frac{3}{12} + \frac{1}{12} = \frac{1}{2}$

· Probabilité d'apparition de 1 :  $\frac{3}{4} * \frac{2}{3} = \frac{6}{12} = \frac{1}{2}$

$$E' = \frac{1}{2} + \frac{1}{2} = 1$$

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

La réponse correcte est :

10

**Question 14**

Correct

Note de 1,00 sur 1,00

## 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.

On peut considérer que le chiffrement est parfait.

- ☐ Vrai
- ☒ Faux ✓

La réponse correcte est « Faux ».

**Question 15**

Correct

Note de 2,00 sur 2,00

## Sécurité réseau Question 1

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

# addresses

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	2230	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	195.55.55.1	3	3	195.55.55.1	195.5.5.2	1040	53

Laquelle de ces affirmations est vraie ?

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

Votre réponse est correcte.

La réponse correcte est :

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

#### Question 16

Correct

Note de 2,00 sur 2,00

#### Sécurité réseau Question 2

On suppose que le pare-feu accepte le Packet#3.

Parmi les affirmations suivantes, indiquer quelle est celle qui est fausse :

- ☐ a. La table de translation contient la translation d'adresse suivante :  
IP privée : 192.168.4.1 --> IP publique : 195.5.5.1
- ☐ b. Le Packet#3 est la réponse à la demande de connexion (paquet SYN) correspondant au Packet#2.
- ☐ c. Le Packet#3 est un message SYN-ACK envoyé par le serveur web d'adresse IP 195.5.5.1.
- ☒ d. La table de translation contient la translation de port suivante : ✓  
Port privé : 2240 --> Port public : 103

Votre réponse est correcte.

Les réponses correctes sont :

Le Packet#3 est la réponse à la demande de connexion (paquet SYN) correspondant au Packet#2., La table de translation contient la translation de port suivante :

Port privé : 2240 --> Port public : 103

**Question 17**

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 3 :

Suite de la question précédente

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

Veuillez choisir une réponse.

- ☐ Vrai
- ☒ Faux ✓

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

La réponse correcte est « Faux ».

**Question 18**

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 4 :

Suite de la question précédente

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	Established	Full connection Default 3600s

Veuillez choisir une réponse.

- ☐ Vrai
- ☒ Faux ✓

La réponse correcte est « Faux ».

**Question 19**

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 5 :

Suite de la question précédente

Le pare-feu accepte le paquet Packet#6

Veuillez choisir une réponse.

- ☒ Vrai ✓
- ☐ Faux

La réponse correcte est « Vrai ».

**Question 20**

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 6 :

Suite de la question précédente

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 paquet va être bloqué
- ☐ b. Le pare-feu va générer un paquet ICMP et l'envoyer à l'adresse IP 155.5.5.2 sur le port 53
- ☐ c. Le pare-feu va créer une nouvelle entrée dans sa table de session
- ☒ 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 correcte.

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.

Voir le slide 54 du cours "Sécurité réseau 1" pour plus d'explication.

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 21**

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 7 :

Suite de la question précédente

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. Slow Loris
- ☒ b. Black Nurse ✓
- ☐ c. Smurf
- ☐ d. Syn-Flooding

Votre réponse est correcte.

La réponse correcte est :

Black Nurse

**Question 22**

Correct

Note de 1,00 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.
- 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.

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 ?

- ☐ a. Radiologue
- ☐ b. Pédiatre
- ☐ c. Ophtalmologue
- ☐ d. Stagiaire\_radiologue
- ☐ e. Stagiaire\_pédiatre
- ☐ f. Stagiaire\_ophtalmologue
- ☐ g. Infirmier
- ☒ h. Aucun ✓

Votre réponse est correcte.

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 23

Correct

Note de 1,00 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 correcte.

Les réponses correctes sont :

Médecin,

Stagiaire\_radiologue



**Question 24**

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 25**

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 26**

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 27**

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.

La réponse correcte est :

&lt;modifier, dossier\_patient\_radiologie&gt;

**Question 28**

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 :

&lt;créer, dossier\_patient\_pédiatrie&gt; ,

&lt;lire, dossier\_patient\_pédiatrie &gt;

**Question 29**

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.

- ☒ 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 :

&lt;créer, dossier\_patient\_radiologie&gt; ,

&lt;lire, dossier\_patient\_radiologie&gt; ,

&lt;créer, dossier\_patient\_pédiatrie&gt; ,

&lt;lire, dossier\_patient\_pédiatrie &gt; ,

&lt;créer, dossier\_patient\_ophtalmologie&gt; ,

&lt;lire, dossier\_patient\_ophtalmologie &gt;

**Question 30**

Correct

Note de 1,00 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. 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
- ☐ b. Une contrainte de séparation des pouvoirs dynamique (DSOD) entre les rôles radiologue et pédiatre
- ☐ c. Une contrainte de cardinalité sur le nombre de rôles qui peut être affecté au médecin
- ☒ d. Une contrainte de séparation des pouvoirs statique (SSOD) entre les rôles radiologue et pédiatre ✓

Votre réponse est correcte.

La réponse correcte est :

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

**Question 31**

Correct

Note de 1,00 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. Une contrainte de séparation des pouvoirs dynamique (DSOD) entre les rôles stagiaire\_radiologue et stagiaire\_pédiatre ✓
- ☐ b. Une contrainte de séparation des pouvoirs statique (SSOD) entre les rôles stagiaire\_radiologue et stagiaire\_pédiatre
- ☐ c. 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.
- ☐ d. Il est impossible d'exprimer cette contrainte avec le modèle AGLP.

Votre réponse est correcte.

La réponse correcte est :

Une contrainte de séparation des pouvoirs dynamique (DSOD) entre les rôles stagiaire\_radiologue et stagiaire\_pédiatre

**Question 32**

Correct

Note de 1,00 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 correcte.

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 33**

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

Votre réponse est correcte.

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

**Question 34**

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

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 35**

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 établit un concept de "session" permettant d'éviter la transmission des paramètres cryptographiques à chaque paquet
- ☐ c. Ce mode permet d'assurer l'intégrité des paquets IP transmis entre correspondants du même réseau virtuel
- ☐ d. Ce mode permet de chiffrer le trafic IP entre deux correspondants à travers l'Internet

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 36**

Correct

Note de 1,00 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. L'autorité de certification doit supprimer le certificat lorsqu'il a été révoqué.
- ☐ b. Chaque certificat possède une date d'expiration. L'autorité de certification doit supprimer le certificat lorsque la date d'expiration est atteinte.
- ☒ c. L'autorité de certification peut décider de révoquer un certificat. Le navigateur (browser ou butineur) du client doit consulter l'autorité de certification pour vérifier que le certificat n'a pas été révoqué. ✓
- ☒ d. 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. ✓

Votre réponse est correcte.

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.