Commencé le	vendredi 16 décembre 2022, 09:30
État	Terminé
Terminé le	vendredi 16 décembre 2022, 11:57
Temps mis	2 heures 27 min
Points	36,25/40,00
Note	**9,06** sur 10,00 (**90,63**%)

Question **1**

Correct

Note de 1,00 sur 1,00

Sélectionner l'affirmation correcte parmi les affirmations suivantes :

a. L'IPS ne sait pas traiter les flux réseau

b. Le firewall et l'IPS ne peuvent être déployés l'un sans l'autre

c. Le firewall réseau détecte les malware contrairement à l'IPS

d. L'IPS se base sur le firewall pour détecter et réagir aux flux malveillants

e. Le firewall et l'IPS bloquent certains flux conformément à la politique de sécurité ✔

Votre réponse est correcte.

La réponse correcte est :
Le firewall et l'IPS bloquent certains flux conformément à la politique de sécurité

Question **2**

Correct

Note de 1,00 sur 1,00

La translation d'adresses peut être remplacée par le déploiement d'un IDS.

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

Question **3**

Correct

Note de 1,00 sur 1,00

Le modèle de Bell à Lapadula permet de bloquer les malwares.

Veuillez choisir une réponse.

- Vrai
- Faux ✔

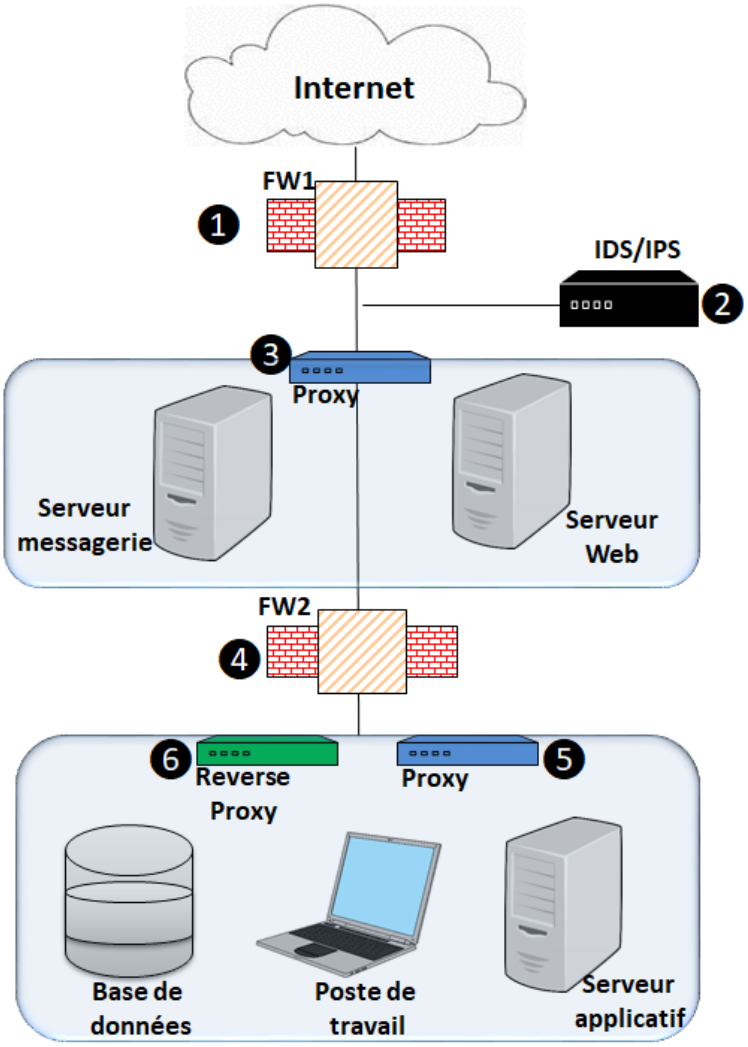
La réponse correcte est « Faux ».

Question **4**

Correct

Note de 1,00 sur 1,00

On considère l'architecture de sécurité suivante :



Quels composants contribuant à cette architecture de sécurité sont mal placés ?

- a. 5 et 6 ✔
- b. 3 et 5
- c. 1 et 2
- d. 2 et 4
- e. 1 et 4

Votre réponse est correcte.

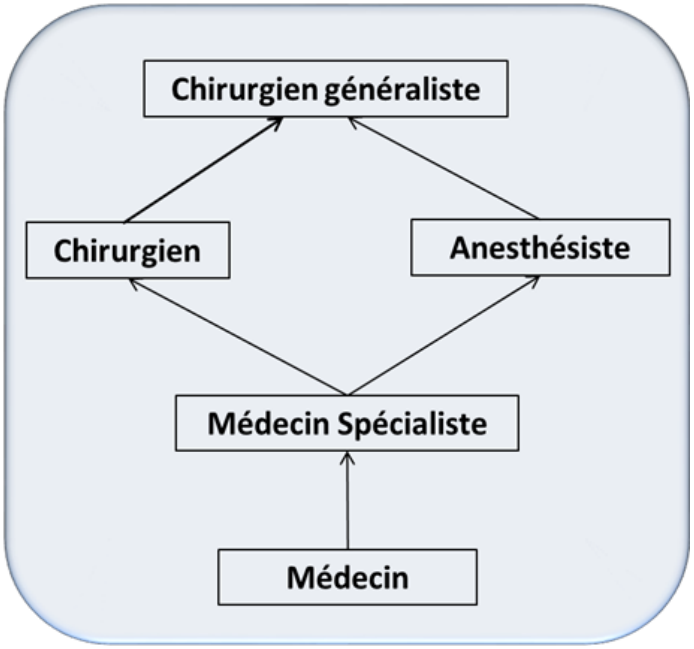
La réponse correcte est :
5 et 6

Question **5**

Terminé

Note de 0,75 sur 1,00

Soit la hiérarchie de rôles suivante :



Sachant qu'un chirurgien généraliste peut occasionnellement jouer le rôle de Chirurgien et d'anesthésiste, et qu'il ne peut cumuler les permissions des deux rôles, comment proposeriez-vu de résoudre le problème de cumul qui apparait dans la hiérarchie de rôles qui vous a été proposée ?

Ici, le type de contrôle d'accès est RBAC (donc utilisateur à une session qui à un ou plusieurs rôles et il hérite des permissions de ce rôle). Ici pour résoudre ce problème, il faudrait affecter une contraintes de séparation des pouvoir pour faire en sorte qu'un utilisateur ne puisse pas activer à la fois le rôle de chirurgien et d'anesthésiste. Il faudrait que cette contrainte soit dynamique pour pouvoir permettre à l'utilisateur d'activer un des rôles à la fois dans une session mais pas en même temps.

À NOTER: Il n'y a pas d'endroits pour émettre des hypothèses, donc les voici:

Dans la question 25 pour la dernière commande soit:

login: « 1234 » / pwd: « blabla") 0R ("a"="a

J'ai répondu requête mal formatté car il y a un 0 à la place du O dans le "OR". Je ne suis pas sur si c'est voulu donc je précise que je l'ai remarqué et que c'est pour cela que j'ai dit requête mal formé.

Aussi, pour la série de questions 19 à 23, je considère que, comme dans le graphique des notes à la page 25 du chp 10, le mémoire est lu dans le sens inverse du sens dans lequel on écrit. C'est pour cela que pour toutes ces questions, j'ai mit l'ordre inverse de l'ordre d'écriture.

Pour la question 33, le state ne match pas related (politique de forward vers l'ext sur le port 53 accepte juste si c'est related et ne match pas car nouvelle requête) donc on drop le paquet selon la politique par default. Ainsi, pour la question 34, le paquet sera drop puisque le payload ne correspond pas à une requête UDP qui a été accepté.

Les questions ci-dessus dépendent l'une de l'autre et j'ai suivi mon raisonnement pour ces dernières. Je veux tout de même l'expliquer puisque je ne veux pas qu'une erreur dans une question initial ou un raisonnement sur lequel ce battit le reste influence toutes mes réponses. Je ne pense pas que ce soit le cas, je pense avoir raison sinon je n'aurais pas mit ces réponses mais je prend tout de même cette précaution puisque beaucoup de question sont construit l'une sur l'autre ou comporte le même genre de raisonnement (et même erreur si jamais) et je ne voudrais pas être pénalisé dans toutes ces questions si jamais. Sur ce, bonne vacances et merci pour la session!

Réponse en deux parties :

(1) Il faut supprimer le lien hiérarchique entre le rôle chirurgien et chirurgien généraliste ou alors supprimer le lien hiérarchique entre le rôle anesthésiste et chirurgien généraliste.

(2) Il faut créer une règle de separation of duty de type dynamique (DSOD) entre les rôles anesthésiste et chirurgien

Commentaire :
Incomplet. Il faut aussi enlever un des deux héritages

Question **6**

Correct

Note de 1,00 sur 1,00

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

a. Aucune de ses réponses, l'informatique quantique n'a pas d'effet sur les algorithmes de chiffrement symétrique

b. L'algorithme de Pollard

c. L'algorithme de Shor

d. L'algorithme de Grover✔

Votre réponse est correcte.

La réponse correcte est :
L'algorithme de Grover

Question **7**

Correct

Note de 1,00 sur 1,00

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

a. Ce mécanisme est désormais natif dans la plupart des systèmes d'exploitation ✔

b. Quand le programme est compilé

c. Quand le programme est exécuté

d. Quand le programmeur écrit le programme

Votre réponse est correcte.

La réponse correcte est :
Ce mécanisme est désormais natif dans la plupart des systèmes d'exploitation

Question **8**

Correct

Note de 1,00 sur 1,00

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

a. Quand le programmeur écrit le programme

b. Quand le programme est exécuté

c. Ce mécanisme est désormais natif dans la plupart des systèmes d'exploitation

d. Quand le programme est compilé ✔

Votre réponse est correcte.

La réponse correcte est :
Quand le programme est compilé

Question **9**

Correct

Note de 2,00 sur 2,00

Le navigateur (ou butineur) d'un utilisateur (le client) établit une connexion avec un serveur via le protocole SSL-TLS.
Remettre dans l'ordre les étapes réalisées entre le client et le serveur pour établir cette connexion :

Le serveur envoie son certificat au client.	Etape 2 ✔
Le navigateur du client vérifie que la signature du certificat est valide et correspond à une autorité présente dans la base des autorités de certification du client.	Etape 3 ✔
Le navigateur du client envoie au serveur la clé symétrique chiffrée avec la clé publique contenue dans le certificat du serveur.	Etape 7 ✔
Le navigateur du client consulte l'autorité signataire du certificat pour vérifier que le certificat n'est pas révoqué.	Etape 4 ✔
Le navigateur du client génère une clé de chiffrement symétrique.	Etape 5 ✔
Le navigateur du client envoie au serveur une demande de connexion par SSL-TLS.	Etape 1 ✔
Le serveur utilise sa clé privée pour déchiffrer la clé symétrique envoyée par le navigateur du client.	Etape 8 ✔
Le navigateur du client chiffre la clé symétrique en utilisant la clé publique contenue dans le certificat du serveur.	Etape 6 ✔

Votre réponse est correcte.

La réponse correcte est :
Le serveur envoie son certificat au client. → Etape 2,

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

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

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

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

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

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

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

Question **10**

Terminé

Note de 2,00 sur 2,00

Entropie d'une source Question 1 :

Soit p une variable qui peut varier de 0 à 1

On considère une source S qui génère des chaînes de bits (0 ou 1) de la façon suivante :

Si la position du bit dans la chaîne est impaire, alors il y a 50% de chance que le bit soir un 0 et 50% de chance que ce soit un 1.

Si la position du bit dans la chaîne est paire, alors : (1) si le bit précédent dans la chaîne est un 0, la probabilité que le bit soit un 0 est égale à p et la probabilité que le bit soit un 1 est égale à (1 – p) et (2) si le bit précédent dans la chaîne est un 1, la probabilité que le bit soit un 1 est égale à p et la probabilité que le bit soit un 0 est égale à (1 – p).

Quelle est l'entropie fréquentielle caractère par caractère de la source S ? Justifier votre calcul.

Il s'agit de calculer la fréquence d'apparition des 0 et des 1 dans la chaîne générée par la source S.

La séquence « 00 » apparait dans 0,5 * p = 0.5p des cas.

La séquence « 01 » apparait dans 0,5 * (1-p) = 0.5 - 0.5p des cas.

La séquence « 10 » apparait dans 0,5 * (1-p) = 0.5 - 0.5p des cas.

La séquence « 11 » apparait dans 0,5 * p = 0.5p des cas.

La probabilité d'apparition d'un 0 dans la chaîne est donc de :

(0.5p * 2 + 0.5 - 0.5p + 0.5 - 0.5p) / 2 = 0,5

Et la probabilité d'apparition d'un 1 dans la chaîne est donc également de 0,5.

L'entropie caractère par caractère de la source S est donc de 1 bit.

Réponse question 1 :

Il s'agit de calculer la fréquence d'apparition des 0 et des 1 dans la chaîne générée par la source S.

La probabilité d'apparition de séquence « 00 » est (0,5 * p).

La probabilité d'apparition de séquence « 01 » est 0,5 * (1 – p)

La probabilité d'apparition de séquence « 10 » est 0,5 * (1 - p)

La probabilité d'apparition de séquence « 11 » est (0,5 * p)

La probabilité d'apparition d'un 0 dans la chaîne est donc de :

(2 * (0,5 * p) + 0,5 * (1 – p) + 0,5 * (1 – p)) / 2 = (p + (1- p)) / 2 = 1/2

Et la probabilité d'apparition d'un 1 dans la chaîne est donc également de 0,5.

L'entropie fréquentielle caractère par caractère de la source S est donc de 1 bit.

Commentaire :

Question **11**

Correct

Note de 1,00 sur 1,00

Entropie d'une source Question 2 :

Suite de la question précédente

Pour quelle valeur de p la source S est-elle markovienne ?

a. La source S est toujours markovienne quelle que soit la valeur de p

b. p = 1

c. p = 0

d. La source S n'est jamais markovienne quelle que soit la valeur de p

e. p = 0,5 ✔

Votre réponse est correcte.

La réponse correcte est :
p = 0,5

Question **12**

Correct

Note de 1,00 sur 1,00

Entropie d'une source Question 3 :

Suite de la question précédente

On considère la source S^2 identique à la source S mais qui génère des blocs de 2 bits (digramme).

La source S^2 est toujours markovienne quelle que soit la valeur de p.

Veuillez choisir une réponse.

Vrai ✔

Faux

La réponse correcte est « Vrai ».

Question **13**

Correct

Note de 1,00 sur 1,00

Entropie d'une source Question 4 :

Suite de la question précédente

On considère la source S^2 identique à la question précédente.

Pour quelle valeur de p, l'entropie de S^2 est égale à 1 (plusieurs réponses possibles) :

- a. L'entropie de S est toujours égale à 1 quelle que soit la valeur de p
- b. p = 0,5
- c. p = 0 ✔
- d. L'entropie de S n'est jamais égale à 1 quelle que soit la valeur de p
- e. p = 1 ✔

Votre réponse est correcte.

Les réponses correctes sont :
p = 0,

p = 1

Question **14**

Correct

Note de 1,00 sur 1,00

Entropie d'une source Question 5 :

Suite de la question précédente

On considère la source S^2 identique à la question précédente.

Pour quelle valeur de p, l'entropie de S^2 est égale à 2 (plusieurs réponses possibles) :

- a. L'entropie de S n'est jamais égale à 2 quelle que soit la valeur de p
- b. p = 0,5 ✔
- c. p = 0
- d. L'entropie de S est toujours égale à 2 quelle que soit la valeur de p
- e. p = 1

Votre réponse est correcte.

La réponse correcte est :
p = 0,5

Question **15**

Correct

Note de 1,00 sur 1,00

Entropie d'une source Question 6 :

Suite de la question précédente

On considère la source S^2 identique à la question précédente.

Quelle est l'entropie du langage associé à la source S ?

a. Egale à l'entropie de la source S^2

b. Egale à l'entropie fréquentielle caractère par caractère de la source S

c. Aucune de ces réponses

d. Egale à la moitié de l'entropie de la source S^2✔

Votre réponse est correcte.

Réponse :

On a H_L(S) = lim{b --> infini} (H(S^b) / b)

Si b = 2n (b est pair) alors H(S^2n) = n H(S^2) car S^2 est markovienne.

H_L(S) = lim{2n --> infini} (n H(S^2) / 2n) = H(S^2) / 2

Si b = 2n + 1 (b est impair) alors H(S^b) = n H(S^2) + 1

H_L(S) = lim{2n+1 --> infini} ((n H(S^2) + 1) / (2n + 1))

= lim (2n+1 --> infini} (n H(S^2) / (2n + 1)) + lim (2n+1 infini} (1 / (2n + 1))

Donc H_L(S) = H(S^2) / 2 + 0 = H(S^2) / 2

La réponse est donc : H_L(S) = H(S^2) / 2

La réponse correcte est :
Egale à la moitié de l'entropie de la source S^2

Question **16**

Terminé

Note de 2,00 sur 2,00

Entropie d'une source Question 7 :

Suite de la question précédente

On considère la source S^2 identique à la question précédente. On note H(S^2) l'entropie de cette source.

On considère une deuxième source S1 qui génère un 0 avec une probabilité p et un 1 avec une probabilité (1 – p). On note H(S1) l'entropie de cette source.

Montrer que H(S^2) = 1 + H(S1)

Indication :

- Donner l'entropie de H(S1) en fonction de p
- Donner l'entropie de H(S^2) en fonction de p
- En déduire le résultat demandé

Rappel :

- Log2 (a * b) = Log2 (a) + Log2 (b)
- Log2 (a / b) = Log2 (a) – Log2 (b)

Tout ci dessous sont des log2

H(S1) = p log(1/p) + (1-p)log(1/1-p)

= p(log(1) - log(p)) + (1-p)(log(1) - log(1-p))

= -p * log(p) + (1-p)(-log(1-p))

H(S2) = 2 x 0.5p log(1/0.5p) + 2x(0.5 - 0.5p)log(1/0.5 - 0.5p)

= p*log(2/p) + (1 - p)(log(2 / (1- p))

= p - p*log(p) + (1-p)(1 - log(1-p)))

= p - p*log(p) + 1 - p + (1-p)(-log(1-p)

= -p * log(p) + (1-p)(-log(1-p)) + 1

H(S^2) = 1 + H(S1)

CQFD

Réponse :

Entropie de S1 : p * Log2(1/p) + (1 – p) * Log2(1 – p)

Entropie de S^2 :

L'alphabet de la source S^2 est {00, 01, 10, 11}

On a :

P(S^2 = « 00 ») = 0,5 * p

P(S^2 = « 01 ») = 0,5 * (1 – p)

P(S^2 = « 10 ») = 0,5 * (1 – p)

P(S^2 = « 11 ») = 0,5 * p

En appliquant la formule de Shannon, on a :

H(S^2) = (0,5 * p) Log2(1/(0,5*p)) + 0,5 * (1 – p) Log2(1/(0,5*(1 - p))) + (+ 0,5 * (1 – p) Log2(1/(0,5*(1 - p))) + (0,5 * p) Log2(1/(0,5*p))

Donc H(S^2) = p Log2(1/(0,5*p)) + (1 – p) Log2(1/(0,5*(1-p)))

H(S^2) = p Log2(1/0,5) + p Log2(1/p) + (1 – p) Log2(1/0,5) + (1 –p) Log2(1/(1-p))

H(S^^2) = p Log2(2) + (1-p) Log2(2) + p Log2(1/p) + (1 –p) Log2(1/(1-p))

Donc H(S^2) = 1 + H(S1)

Commentaire :

Question **17**

Correct

Note de 1,00 sur 1,00

Sécurité logiciel Question 1 :

On considère le programme « getshell.c » suivant :

```
#include <stdio.h>
#include  <stdlib.h>

int main(){
     long val=0x41414141;
     char buf[5];

     printf("Changer la valeur de val de 0x41414141 à 0xdeadbeef !\n");
     print("Tenter votre chance : ");
     scanf("%9s",&buf);

     printf("val : 0x%08x\n",val);

     if(val==0xdeadbeef){
         setreuid(geteuid(),geteuid());
         system("/bin/sh ");
     }
     else{
         printf("Perdu !\n");
         exit(1);
     }
     return 0;}
```

Quelques indications :

La fonction « scanf » permet la saisie de données formatées, qu'il s'agisse de lettres, de chiffres ou de chaînes de caractère.

L'instruction « printf("val : 0x%08x\n",val) ; » permet l'affichage de 8 caractères au format hexadécimal.

L'instruction « setreuid(geteuid,geteuid) » sert à définir l'ID utilisateur réel et l'ID utilisateur effectif du processus appelant. Dans ce cas, le processus s'exécutera avec l'euid du serveur.

Le caractère « A » en hexadécimal vaut 0x41

Quelle vulnérabilité identifiez-vous dans ce programme ?

- a. Heap overflow
- b. Format string vulnerability
- c. Stack overflow ✔
- d. Fuite de mémoire

Votre réponse est correcte.

La réponse correcte est :
Stack overflow

Question **18**

Correct

Note de 1,00 sur 1,00

Sécurité logiciel Question 2 :

Suite de la question précédente

Vous exécutez la commande suivante :

python -c 'print "BBBB" ' | /getshell

Vous obtenez le résultat suivant :

val = 0x41414141
Perdu !

Veuillez choisir une réponse.

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question **19**

Correct

Note de 1,00 sur 1,00

Sécurité logiciel Question 3 :

Suite de la question précédente

Vous exécutez la commande suivante :

python -c 'print "AAAAABCDE" ' | /getshell

Quelle est valeur de val après l'exécution de cette commande ?

a. val = 0x42434445
b. val = 0x45444342 ✔
c. val = 0xefbeadde
d. val = 0xdeadbeef

Votre réponse est correcte.

La réponse correcte est :
val = 0x45444342

Question **20**

Correct

Note de 1,00 sur 1,00

Sécurité logiciel Question 4 :

Suite de la question précédente

Vous exécutez la commande suivante :

python -c ‘print “AAAAAEDCB” ’ | /getshell

Quelle est valeur de val après l’exécution de cette commande ?

- a. val = 0x42434445 ✔
- b. val = 0xdeadbeef
- c. val = 0xefbeadde
- d. val = 0x45444342

Votre réponse est correcte.

La réponse correcte est :
val = 0x42434445

Question **21**

Correct

Note de 1,00 sur 1,00

Sécurité logiciel Question 5 :

Suite de la question précédente

Vous exécutez la commande suivante :

python -c ‘print “AAAAA” + “\xde\ad\xbe\ef” ’ | /getshell

Quelle est valeur de val après l’exécution de cette commande :

- a. val = 0x45444342
- b. val = 0x42434445
- c. val = 0xefbeadde ✔
- d. val = 0xdeadbeef

Votre réponse est correcte.

La réponse correcte est :
val = 0xefbeadde

Question **22**

Correct

Note de 1,00 sur 1,00

Sécurité logiciel Question 6 :

Suite de la question précédente

Vous exécutez la commande suivante :

python -c 'print "AAAAA" + "\xef\be\xad\de" ' | /getshell

Quelle est valeur de val après l'exécution de cette commande ?

- a. val = 0x45444342
- b. val = 0x42434445
- c. val = 0xefbeadde
- d. val = 0xdeadbeef ✔

Votre réponse est correcte.

La réponse correcte est :
val = 0xdeadbeef

Question **23**

Correct

Note de 1,00 sur 1,00

Sécurité logiciel Question 7 :

Suite de la question précédente

Que se passe-t-il lorsque vous exécutez la commande suivante :

python -c 'print "AAAAA" + "\xef\be\xad\de" ' | /getshell

- a. Vous obtenez un shell avec les droits du serveur ✔
- b. Le message "Perdu !" s'affiche
- c. Le message "Gagné !" s'affiche
- d. Segmentation fault

Votre réponse est correcte.

La réponse correcte est :
Vous obtenez un shell avec les droits du serveur

Question **24**

Correct

Note de 1,00 sur 1,00

Injection SQL Question 1 :

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 et la base de données

b. La table visée, la base de données et le système de gestion de base de données (SGBD) qui gère la table

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

d. La table visée

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 **25**

Partiellement correct

Note de 1,50 sur 2,00

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 :

login : « 1234 » / pwd : « blabla OR 1=1 »	Requête mal formée	✗
login: « 1234 » / pwd: « blabla") OR (1=1 OR pwd = "blabla »	Authentification contournée	✓
login: « 1234 » / pwd: « blabla") OR (1=1 »	Requête mal formée	✓
login: « 1234 » / pwd: « blabla") 0R ("a"="a »	Requête mal formée	✗

Votre réponse est partiellement correcte.

Vous en avez sélectionné correctement 2.

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") 0R ("a"="a") ;

Requête bien formée et WHERE évalué à vrai = authentification contournée

La réponse correcte est :
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,

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

login: « 1234 » / pwd: « blabla") 0R ("a"="a » → Authentification contournée

Commentaire :
Réévaluation de la question

Question **26**

Correct

Note de 2,00 sur 2,00

Injection SQL Question 3 :

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

```
UPDATE table_name
```

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

```
WHERE [condition];
```

Par exemple :

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

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

Pour cela, le client sélectionne d'abord l'identificateur du compte cpt1 dans une liste déroulante et ensuite l'identificateur du compte ctp2 la même liste déroulante.

Le client saisit ensuite le montant à transférer au clavier.

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

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

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

On suppose que vous avez deux comptes « 11111 » et « 22222 ».

On suppose que le solde initial du compte « 11111 » est de 100$.

On suppose que le solde initial du compte « 22222 » est de 200$.

Quelle attaque vous permet de fixer le solde de votre compte « 11111 » à un montant de 100000$, sans qu'aucun autre de vos comptes ne soit débité.

a. Choisir cpt1 = « 11111 » et cpt2 = « 22222 » et montant = « Solde_compte + 100000 »

b. Choisir cpt1 = « 11111 » et cpt2 = « 11111 » et montant = « Solde_compte + 500000 »

c. Choisir cpt1 = « 11111 » et cpt2 = « 11111 » et montant = « (Solde_compte – 100000) » ✔

d. Choisir cpt1 = « 11111 » et cpt2 = « 11111 » et montant = « Solde_compte - 100000 »

Votre réponse est correcte.

Réponse 1 : cpt1 = 100000 / cpt2 = 100200

Réponse 2 : cpt1 = -300000$

Réponse 3 : cpt1 = 100000$

Réponse 4 : cpt1 = 150000$

La réponse correcte est :
Choisir cpt1 = « 11111 » et cpt2 = « 11111 » et montant = « (Solde_compte – 100000) »

Question **27**

Incorrect

Note de 0,00 sur 1,00

Injection SQL : Question 4

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

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

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

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

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

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

Votre réponse est incorrecte.

La réponse correcte est :
Les trois réponses ci-dessus permettent d'accéder au compte 12345

Question **28**

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 1 :

La translation d'adresses sert à :

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

Votre réponse est correcte.

La réponse correcte est :
Gérer la pénurie d'adresses

Question **29**

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

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

Votre réponse est correcte.

La réponse correcte est :
Le pare-feu bloque le Packet#1 et accepte le Packet#2

Question **30**

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.

Quelle est la table de translation correspondant à cette situation ?

a. IP privée : 192.168.1.1 --> IP publique : 195.5.5.1
Port privé : 2230 --> Port public : 1030

b. IP privée : 192.168.4.1 --> IP publique : 195.5.5.1 ✔
Port privé : 2240 --> Port public : 1030

c. IP privée : 192.168.1.1 --> IP publique : 195.5.5.1
Port privé : 2230 --> Port public : 80

d. IP privée : 192.168.4.1 --> IP publique : 195.5.5.1
Port privé : 2240 --> Port public : 80

Votre réponse est correcte.

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

La réponse correcte est :

IP privée : 192.168.4.1 --> IP publique : 195.5.5.1
Port privé : 2240 --> Port public : 1030

Question **31**

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 4 :

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 **32**

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 5 :

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 **33**

Incorrect

Note de 0,00 sur 1,00

Sécurité réseau Question 6 :

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 **34**

Incorrect

Note de 0,00 sur 1,00

Sécurité réseau Question 7 :

Suite de la question précédente

On suppose que le pare-feu accepte le paquer 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 accepter le paquet et le transférer à l'adresse IP 192.168.4.1 sur le port 3535

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 créer une nouvelle entrée dans sa table de session

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.

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 **35**

Correct

Note de 1,00 sur 1,00

Sécurité réseau Question 8 :

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

Votre réponse est correcte.

La réponse correcte est :
Black Nurse