Commencé le	mercredi 3 mai 2023, 00:11
État	Terminé
Terminé le	mercredi 3 mai 2023, 00:18
Temps mis	7 min 4 s
Points	16,00/18,00
Note	**8,89** sur 10,00 (**88,89**%)

Question **1**

Correct

Note de 1,00 sur 1,00

Comment l'utilisation de certificats permet l'authentification des sites web ?

Veuillez choisir une réponse.

a. La signature numérique du certificat valide le champ CN (l'adresse du site) ✔

b. Le certificat permet l'utilisation d'un algorithme à clé publique

c. Il est très difficile pour un pirate d'avoir accès au certificat

d. Le protocole SSL/TLS assure la confidentialité des informations

e. L'utilisation de certificat n'a rien à voir avec l'authentification

Votre réponse est correcte.

La réponse correcte est : La signature numérique du certificat valide le champ CN (l'adresse du site)

Question **2**

Incorrect

Note de 0,00 sur 1,00

Laquelle de ces méthodes d'authentification sur une application Web représente le risque le plus élevé en terme d'exposition à un scénario de piratage de l'externe (via Internet).

Veuillez choisir une réponse.

a. Le code usager et le mot de passe sont vérifiés par le serveur Web en accédant à une base de données de hachés cryptographiques d'usagers stockée sur la BD relationnelle de l'application Web ✖

b. Le code usager et mot de passe sont vérifiés par le serveur Web en utilisant le fichier /etc/shadow stocké sur le serveur Web

c. Le code usager et le mot de passe sont envoyés à un serveur d'authentification qui répond avec un identificateur de session unique (« session ID ») s'ils sont valides

d. Le code usager et mot de passe sont envoyés tels quels au serveur de BD relationnelle pour ouvrir une session SQL

Votre réponse est incorrecte.

La réponse correcte est : Le code usager et mot de passe sont envoyés tels quels au serveur de BD relationnelle pour ouvrir une session SQL

Question **3**

Correct

Note de 1,00 sur 1,00

Laquelle de ces méthodes ne constitue pas une méthode de prévention des erreurs d'injection de SQL

Veuillez choisir une réponse.

a. L'utilisation d'instructions GRANT et REVOKE pour contrôler l'accès à la base de données ✔

b. L'utilisation de méthodes ou fonctions de filtrage des entrées venant des usagers

c. L'utilisation de méthodes et fonctions directement implémentés sur le serveur de BD (« stored procedures »)

d. L'utilisation d'un détecteur d'intrusion pouvant détecter les chaînes susceptibles d'être utilisés par une attaque d'injection de SQL

Votre réponse est correcte.

La réponse correcte est : L'utilisation d'instructions GRANT et REVOKE pour contrôler l'accès à la base de données

Question **4**

Correct

Note de 1,00 sur 1,00

Laquelle de ces méthodes de générations de jeton de session (« session ID ») est préférable en terme de sécurité

Veuillez choisir une réponse.

a. Un jeton de 10 caractères imprimables, choisis au hasard parmi les lettres majuscules et minuscules sans accent et des chiffres de 0 à 9.

b. Un nombre choisi au hasard entre 1 et 100 milliards, codé avec un caractère ASCII pour chaque chiffre (0 à 9).

c. Une chaine de 64 bits aléatoires codées avec des 0 et des 1 (en ASCII)

d. Une chaine de 5 mots de la langue anglaise, choisis au hasard dans un dictionnaire de 100 000 mots et séparé par un caractère spécial. ✔

Votre réponse est correcte.

La réponse correcte est : Une chaine de 5 mots de la langue anglaise, choisis au hasard dans un dictionnaire de 100 000 mots et séparé par un caractère spécial.

Question **5**

Correct

Note de 1,00 sur 1,00

Quel type d'attaque XSS (cross-site scripting) est la plus dangereuse et pourquoi ?

Veuillez choisir une réponse.

a. XSS non-persistent parce qu'on peut faire activer l'attaque par de l'ingénierie sociale.

b. XSS persistent puisqu'aucune interaction de l'usager n'est requise. ✔

c. XSS persistent parce qu'on peut faire activer l'attaque par de l'ingénierie sociale.

d. XSS non-persistent puisqu'aucune interaction de l'usager n'est requise.

Votre réponse est correcte.

La réponse correcte est : XSS persistent puisqu'aucune interaction de l'usager n'est requise.

Question **6**

Correct

Note de 1,00 sur 1,00

Lequel de ces systèmes n'utilise pas de l'authentification à deux facteurs :

Veuillez choisir une réponse.

a. Un site Web qui demande le nom d'usager et le mot de passe, et ensuite de répondre à une question de sécurité ✔

b. Un ordinateur de bureau qui se débloque seulement lorsqu'on insère une carte à puce et lorsqu'on introduit le bon code usager et mot de passe

c. Un ordinateur portable qui se débloque lorsqu'on passe son doigt sur le lecteur d'empreinte digitale **et** qui nécessite l'introduction d'un mot de passe au démarrage

d. Un site Web qui détecte et reconnait le rythme de frappe au clavier de l'usager (à travers une applet Java sur le fureteur) et qui demande un code à usage unique (« one-time password ») généré sur un téléphone intelligent

Votre réponse est correcte.

La réponse correcte est : Un site Web qui demande le nom d'usager et le mot de passe, et ensuite de répondre à une question de sécurité

Question **7**

Correct

Note de 1,00 sur 1,00

Quelle est l'utilité de faire de la validation des données saisies sur le client ?

Veuillez choisir une réponse.

a. Permet de détecter des exploits (« shell code ») qui aurait pu être insérés dans les inputs d'usagers

b. Permet de filtrer les injections SQL et les attaques XSS (cross-site scripting). ✔

c. Permet d'améliorer la performance et l'expérience usager pour les usagers non-malveillants.

d. Aucune utilité.

Votre réponse est correcte.

La réponse correcte est : Permet de filtrer les injections SQL et les attaques XSS (cross-site scripting).

Question **8**

Incorrect

Note de 0,00 sur 1,00

Laquelle de ces mesures de remédiation ne permet pas d'empêcher les injections SQL ?

Veuillez choisir une réponse.

a. L'utilisation de pare-feu applicatif spécialisé en application web.

b. L'utilisation de procédures stockées (« stored procedures »).

c. Le filtrage des caractères spéciaux.

d. La limitation des droits de l'application dans la base de données.

e. Le ré-encodage des caractères spéciaux. ✖

Votre réponse est incorrecte.

La réponse correcte est : La limitation des droits de l'application dans la base de données.

Question **9**

Correct

Note de 1,00 sur 1,00

Pourquoi est-il nécessaire de chiffrer les communications d'un site web après l'authentification, même si le contenu du site ne nécessite aucune confidentialité

Veuillez choisir une réponse.

a. Pour préserver la vie privée.

b. Pour garantir la disponibilité.

c. Parce que l'utilisation de SSL/TLS est sécuritaire.

d. Pour éviter l'utilisation de cookies.

e. Certaines informations systèmes comme l'identificateur de session sont sensibles et peuvent transiter dans la communication. ✔

Votre réponse est correcte.

La réponse correcte est : Certaines informations systèmes comme l'identificateur de session sont sensibles et peuvent transiter dans la communication.

Question **10**

Correct

Note de 1,00 sur 1,00

Pourquoi est-il nécessaire d'utiliser une forme de XSS (cross-site scripting) pour voler un cookie ?

Veuillez choisir une réponse.

a. Pour que la requête s'exécute dans le contexte du site web attaquant.

b. Pour que la requête s'exécute dans le contexte du site web à qui appartient le cookie. ✔

c. Pour faciliter l'ingénierie sociale.

d. Pour permettre à l'attaque de faire une attaque d'homme au milieu (man-in-the-middle).

e. Pour outrepasser le chiffrement.

Votre réponse est correcte.

La réponse correcte est : Pour que la requête s'exécute dans le contexte du site web à qui appartient le cookie.

Question **11**

Laquelle de ces méthodes est la plus efficace pour détecter les failles de logique applicatives dans les

Correct

Note de 1,00 sur 1,00

applications web ?

Veuillez choisir une réponse.

a. L'utilisation de pare-feu applicatif spécialisé en application web.

b. La revue manuelle de code. ✔

c. Le filtrage des caractères spéciaux.

d. La limitation des droits de l'application dans la base de données.

e. Le ré-encodage des caractères spéciaux.

Votre réponse est correcte.

La réponse correcte est : La revue manuelle de code.

Question **12**

Correct

Note de 1,00 sur 1,00

Lequel de ces moyens n'est pas adéquat pour implémenter la logique du mécanisme de contrôle d'accès dans une application Web :

Veuillez choisir une réponse.

a. Les commandes grant et revoke sur le serveur de base de données

b. Les permissions d'accès des fichiers HTML sur les répertoires du serveur Web

c. Le code javascript exécuté sur le fureteur du client Web ✔

d. Le code qui s'exécute sur un serveur d'application entre le serveur Web et le serveur de base de données

Votre réponse est correcte.

La réponse correcte est : Le code javascript exécuté sur le fureteur du client Web

Question **13**

Correct

Note de 1,00 sur 1,00

Un hacker souhaite frauder un service Web. Une transaction sur ce site suit le format suivant

GET www.banqueacme.com/transactions/DO?sessionID=8734521203&trans_id=6&value=1000

où la sessionID est le jeton de session qui est inclus dans le cookie du site. Il est possible de changer le paramètre "value" pour payer un montant moins élevé que le montant prévu par l'application. De quel type d'attaque s'agit-il ?

Veuillez choisir une réponse.

a. XSS persistent

b. XSS non persistent

c. Injection SQL

d. CSRF

e. Logique de l'application ✔

Votre réponse est correcte.

La réponse correcte est : Logique de l'application

Question **14**

Correct

Note de 1,00 sur 1,00

Les vulnérabilités d'injection de code SQL dans les applications Web sont un exemple de vulnérabilités du au filtrage déficient des entrées d'usager

Veuillez choisir une réponse.

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question **15**

Correct

Note de 1,00 sur 1,00

L'injection SQL n'est pas un problème si votre mode d'authentification n'utilise pas des requêtes de base de données

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **16**

Correct

Note de 1,00 sur 1,00

Les vulnérabilités de cross-site scripting (XSS) sont un exemple de vulnérabilités du au filtrage déficient des entrées d'usager

Veuillez choisir une réponse.

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question **17**

Correct

Note de 1,00 sur 1,00

L'utilisation de fonctions stockées (« stored procedures ») sur un moteur de base de données peut constituer une contremesure efficace contre les vulnérabilités d'injection de SQL.

Veuillez choisir une réponse.

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question **18**

Correct

Note de 1,00 sur 1,00

Le modèle de sécurité basée sur l'origine de HTTP (« same domain policy ») permet de prévenir le vol de cookie par XSS

Veuillez choisir une réponse.

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

◀ INF4420A H2023 Enregistrement Cours #9 Sécurité Web

Aller à...

Cours Securite Web Capsule 1 Presentation du cours ▶

Commencé le	mercredi 3 mai 2023, 01:08
État	Terminé
Terminé le	mercredi 3 mai 2023, 01:17
Temps mis	9 min 17 s
Points	9,00/9,00
Note	**10,00** sur 10,00 (**100**%)

Question **1**

Correct

Note de 1,00 sur 1,00

Lors d'un débordement de pile (« stack overflow »), que cherche-t-on à écraser ?

Veuillez choisir une réponse.

a. Pointeur d'environnement

b. Argument d'appel de fonction

c. Tampon d'environnement

d. Pointeur de retour ✔

Votre réponse est correcte.

La réponse correcte est : Pointeur de retour

Question **2**

Correct

Note de 1,00 sur 1,00

Lors d'un débordement du tas (« heap overflow »), que cherche-t-on à écraser ?

Veuillez choisir une réponse.

a. Pointeur d'environnement local

b. Argument d'appel de fonction

c. Données stockées en mémoire ✔

d. Pointeur de retour

Votre réponse est correcte.

La réponse correcte est : Données stockées en mémoire

Question **3**

Correct

Note de 1,00

Quelle utilisation de ces fonctions C++ est la plus susceptible d'être vulnérable à une attaque de débordement de mémoire tampon :

Note de 1,00 sur 1,00

Veuillez choisir une réponse.

- a. strcpy (copie la chaine de caractères) ✔
- b. memchr (trouve un caractère dans un bloc de mémoire)
- c. time (affiche le temps)
- d. rand (produit un nombre aléatoire)
- e. strlen (obtenir la longueur d'une chaîne)

Votre réponse est correcte.

La réponse correcte est : strcpy (copie la chaine de caractères)

Question **4**

Correct

Note de 1,00 sur 1,00

Quelle approche n'est pas une technique de protection contre les stack overflow :

Veuillez choisir une réponse.

- a. ALSR (Address space layout randomization)
- b. Les Canaries
- c. ROP (Return Oriented Programming) ✔
- d. Utiliser des langages typés comme JAVA

Votre réponse est correcte.

La réponse correcte est : ROP (Return Oriented Programming)

Question **5**

Correct

Note de 1,00 sur 1,00

Quelle approche n'est pas une technique de protection contre les heap overflow :

Veuillez choisir une réponse.

- a. ALSR (Address space layout randomization)
- b. Les Canaries ✔
- c. ESP (Executable-space protection)
- d. Utiliser des langages typés comme JAVA

Votre réponse est correcte.

La réponse correcte est : Les Canaries

Question **6**

Correct

Note de 1,00 sur 1,00

Que se passe-t-il si un stack overflow parvient à écraser l'adresse de retour mais la nouvelle adresse ne pointe pas vers le shell code :

Veuillez choisir une réponse.

a. Rien, le programme va continuer à s'exécuter

b. En général, cela va causer une erreur « segmentation fault » ✔

Votre réponse est correcte.

La réponse correcte est : En général, cela va causer une erreur « segmentation fault »

Question **7**

Correct

Note de 1,00 sur 1,00

La solution StackShield permet en général d'éviter les « segmentation fault »

Veuillez choisir une réponse.

Vrai ✔

Faux

La réponse correcte est « Vrai ».

Question **8**

Correct

Note de 1,00 sur 1,00

En sécurité informatique le terme « exploit » (en anglais) fait référence à :

Veuillez choisir une réponse.

a. Un outil qui permet de pirater des machines à distance en faisant la reconnaissance sur le réseau et découvrant les vulnérabilités qui y sont présentes

b. Au code machine qui est inséré via le réseau ou via une page Web sur une machine afin de l'infecter

c. Une prouesse informatique réalisée par un pirate qui aurait réussi à devenir « root » sur une machine particulièrement bien protégée

d. Une méthode qui permet de prendre le contrôle d'une machine étant donnée l'existence d'une vulnérabilité sur un de ses logiciels ✔

Votre réponse est correcte.

La réponse correcte est : Une méthode qui permet de prendre le contrôle d'une machine étant donnée l'existence d'une vulnérabilité sur un de ses logiciels

Question **9**

Correct

Note de 1,00 sur 1,00

On considère le programme suivant :

```
void func(int n)
 {          char* chunk = (char*) malloc(32);
            memset(chunk, 'A', n);
            printf("%s\n", chunk);
            free(chunk);
            chunk = NULL; }
int main(int argc, char *argv[])
 {          func(argv[1]);
```

```
return 0;  }
```

Quelle vulnérabilité identifiez-vous dans ce programme ?

Veuillez choisir une réponse.

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

Votre réponse est correcte.

La réponse correcte est : Heap overflow

◀ Support-Séance10-Exercices

Aller à...

Exercice Cours Sécurité Logiciel et des OS ▶

Commencé le	mercredi 3 mai 2023, 01:18
État	Terminé
Terminé le	mercredi 3 mai 2023, 01:34
Temps mis	15 min 47 s
Points	17,00/20,00
Note	**8,50** sur 10,00 (**85**%)

Question **1**

Correct

Note de 1,00 sur 1,00

Laquelle de ces attaques contre un site Web ne pourrait pas être détectée par un pare-feu applicatif combiné à un proxy Web

Veuillez choisir une réponse.

a. Injection SQL

b. Faille de logique dans l'application Web ✔

c. Re-direction vers un site servant du contenu malveillant (p.ex. exploit sur le browser)

d. Attaque de mot de passe par brute force

Votre réponse est correcte.

La réponse correcte est : Faille de logique dans l'application Web

Question **2**

Correct

Note de 1,00 sur 1,00

Un attaquant réalise une attaque de balayage de ports (port scan) avec l'outil nmap sur votre serveur faisant face à l'Internet. Le serveur est protégé par un pare-feu de type filtrage de paquets. Quel(s) service(s) risque(nt) d'être visible(s) à l'attaquant ?

Veuillez choisir une réponse.

a. 22 (ssh)

b. 23 (telnet)

c. 80 (http)

d. 138 (Microsoft Remote Procedure Call DCOM)

e. toutes ces réponses ✔

Votre réponse est correcte.

La réponse correcte est : toutes ces réponses

Question **3**

Correct

Note de 1,00 sur 1,00

Un serveur qui permet à un utilisateur d'accéder depuis Internet aux services internes à une entreprise est un :

Veuillez choisir une réponse.

a. Proxy

b. Reverse proxy ✔

Votre réponse est correcte.

La réponse correcte est :
Reverse proxy

Question **4**

Correct

Note de 1,00 sur 1,00

Lorsqu'un client A réalise une attaque en SYN-flooding sur un serveur B, laquelle de ces affirmations est fausse ?

Veuillez choisir une réponse.

a. A envoie à B des paquets SYN sans envoyer ensuite des paquets ACK

b. A essaye de saturer la pile TCP de B

c. A peut envoyer à B des paquets forgés avec de fausses adresses IP (spoofing)

d. A essaye d'ouvrir un grand nombre de sessions TCP sur le serveur B ✔

Votre réponse est correcte.

La réponse correcte est :
A essaye d'ouvrir un grand nombre de sessions TCP sur le serveur B

Question **5**

Correct

Note de 1,00 sur 1,00

En quoi consiste l'attaque « ping of death » ?

Veuillez choisir une réponse.

a. A envoyer un paquet avec tous les flags TCP positionnés à 1

b. A envoyer un paquet ayant une adresse IP source égale à l'adresse IP destination

c. A envoyer un paquet dont la taille dépasse la taille maximale autorisée (65535 octets) ✔

d. A envoyer des paquets mal fragmentés

Votre réponse est correcte.

La réponse correcte est :
A envoyer un paquet dont la taille dépasse la taille maximale autorisée (65535 octets)

Question **6**

Correct

Note de 1,00 sur 1,00

Parmi les affirmations suivantes, laquelle n'est par un principe de bastionnage d'un serveur proxy ?

Veuillez choisir une réponse.

a. Chaque proxy s'exécute comme un usager non privilégié dans un répertoire privé et sécurisé

b. Bloquer le trafic non chiffré ✔

c. Concevoir chaque module de proxy de façon minimale et sécurisée

d. Installer uniquement les services nécessaires pour l'administration réseau

Votre réponse est correcte.

La réponse correcte est :
Bloquer le trafic non chiffré

Question **7**

Correct

Note de 1,00 sur 1,00

Laquelle de ces réponses constitue le facteur le plus important à considérer lorsqu'on doit prendre la décision de mettre un service dans la DMZ.

Veuillez choisir une réponse.

a. Le débit et la qualité de service

b. La nécessité d'authentifier les usagers accédant aux serveurs

c. La nécessité de donner accès au serveur aux usagers externes (à partir de l'Internet) et un accès administratif aux usagers internes ✔

d. La configuration du détecteur d'intrusion et la capacité de l'attaquant

Votre réponse est correcte.

La réponse correcte est : La nécessité de donner accès au serveur aux usagers externes (à partir de l'Internet) et un accès administratif aux usagers internes

Question **8**

Correct

Note de 1,00 sur 1,00

Laquelle de ces affirmations concernant les pare-feux est correcte :

Veuillez choisir une réponse.

a. Un pare-feu applicatif applique des règles simples sur les en-têtes des paquets IP afin de déterminer lesquels doivent être filtrés

b. Un pare-feu sans mémoire (« stateless ») reconstruit les informations des sessions TCP qui y transitent afin de déterminer si certains paquets ne respectent pas le protocole et ainsi les rejeter

c. Un pare-feu peut être installé sur une machine ayant deux cartes réseaux ou plus ✔

d. Les pare-feux permettent de bloquer les requêtes illégitimes lors d'une attaque de déni de service

Votre réponse est correcte

Votre réponse est correcte.

La réponse correcte est : Un pare-feu peut être installé sur une machine ayant deux cartes réseaux ou plus

Question **9**

Correct

Note de 1,00 sur 1,00

Laquelle de ces phrases constitue une condition nécessaire pour qu'une attaque d'empoisonnement de cache ARP (« ARP Cache Poisoning ») soit réalisée avec succès, c'est-à-dire permettant à Ève d'intercepter le trafic entre Alice et Bob.

Veuillez choisir une réponse.

a. Ève doit connaitre l'adresse Ethernet de l'ordinateur d'Alice ou de Bob

b. Ève doit être dans le même VLAN qu'Alice et Bob ✔

c. Alice doit connaître l'adresse Ethernet de Bob

d. Le logiciel du commutateur n'a pas été mis à jour et contient une vulnérabilité exploitable permettant de réaliser l'attaque

Votre réponse est correcte.

La réponse correcte est : Ève doit être dans le même VLAN qu'Alice et Bob

Question **10**

Correct

Note de 1,00 sur 1,00

L'objectif d'un pare-feu de couche 3 est d'empêcher les attaques de type injection SQL

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

Question **11**

Correct

Note de 1,00 sur 1,00

L'utilisation d'un routeur sans-fils à la maison est un atout en terme de sécurité réseaux parce que :

Veuillez choisir une réponse.

a. Il protège les communications au niveau de la couche 2 entre les machines qui y sont reliées avec des protocoles cryptographiques sécurisés.

b. Certains de ces routeurs ont des fonctionnalités de pare-feu qui permettent de limiter le type de connexion entre l'Internet et les machines internes qui y sont reliés.

c. Il implémente le protocole NAT (Network Address Translation) et attribue des adresses privées aux machines qui y sont reliées.

d. Toutes les réponses ci-dessus sont correctes. ✔

Votre réponse est correcte.

La réponse correcte est : Toutes les réponses ci-dessus sont correctes.

Question **12**

Correct

Note de 1,00 sur 1,00

Un pare-feu considérant l'état (« stateful firewall ») bloquera un paquet ACK qui n'est pas précédé par un paquet SYN.

Veuillez choisir une réponse.

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question **13**

Correct

Note de 1,00 sur 1,00

Dans un pare-feu à état comme NetFilter, on ne peut pas définir des règles de filtrage à état sur des protocoles sans état comme UDP

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **14**

Correct

Note de 1,00 sur 1,00

Un pare-feu applicatif bloque automatiquement toutes les attaques de type « faute de logique applicative ».

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **15**

Correct

Note de 1,00 sur 1,00

Le pare-feu Netfilter utilise le concept de chaîne. Quelle chaine n'est pas une chaine définie par défaut dans Netfilter ?

Veuillez choisir une réponse.

- a. TRANSFERT ✔
- b. FORWARD
- c. OUTPUT
- d. INPUT

Votre réponse est correcte.

La réponse correcte est :

La réponse correcte est :
TRANSFERT

Question **16**
Incorrect
Note de 0,00 sur 1,00

Sous Netfilter, lorsque la chaine PREROUTING est utilisée, le pare-feu applique au paquet le transfert d'adresse (NAT) avant d'appliquer les règles de filtrage

Veuillez choisir une réponse.
- Vrai
- Faux ✖

La réponse correcte est « Vrai ».

Question **17**
Correct
Note de 1,00 sur 1,00

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

Veuillez choisir une réponse.
- a. Le pare-feu applique le transfert d'adresse sur l'adresse destination du paquet
- b. Le pare-feu applique le transfert d'adresse sur l'adresse source du paquet ✔

Votre réponse est correcte.

La réponse correcte est :
Le pare-feu applique le transfert d'adresse sur l'adresse source du paquet

Question **18**
Incorrect
Note de 0,00 sur 1,00

Lequel de ces moyens d'accès à Internet par un utilisateur à la maison représentent un plus grand risque de sécurité en termes de disponibilité :

Veuillez choisir une réponse.
- a. Accès sur un laptop avec une clé USB via le réseau cellulaire 3G ou LTE
- b. Accès sur un laptop branché par réseau sans-fils local (Wifi) chiffré sur un « routeur » maison branché à une ligne téléphonique ADSL
- c. Accès via un modem câble branché sur le réseau de cable-distribution (câble de télévision) ✖
- d. Accès sur un laptop avec un modem téléphonique

Votre réponse est incorrecte.

La réponse correcte est : Accès sur un laptop avec une clé USB via le réseau cellulaire 3G ou LTE

Question **19**

Lequel de ces moyens d'accès à Internet par un utilisateur à la maison représentent un plus grand risque de

Correct

Note de 1,00 sur 1,00

sécurité en termes de confidentialité :

Veuillez choisir une réponse.

a. Accès sur un laptop avec une clé USB via le réseau cellulaire 3G ou LTE

b. Accès sur un laptop branché par réseau sans-fils local (Wifi) chiffré sur un « routeur » maison branché à une ligne téléphonique ADSL

c. Accès via un modem câble branché sur le réseau de cablo-distribution (câble de télévision) ✔

d. Accès sur un laptop avec un modem téléphonique

Votre réponse est correcte.

La réponse correcte est : Accès via un modem câble branché sur le réseau de cablo-distribution (câble de télévision)

Question **20**

Non répondue

Noté sur 1,00

Il existe des routeurs qui incluent des fonctions de filtrage réseau. On parle alors de routeur filtrant.

Quelle est la principale différence entre un pare-feu et un routeur filtrant ?

◀ Support-Séance11-Exercices-Corrigé

Aller à...

Exercice Cours Sécurité Réseau 1 ▶

Commencé le	samedi 29 avril 2023, 20:01
État	Terminé
Terminé le	samedi 29 avril 2023, 20:12
Temps mis	11 min 39 s
Points	11,00/15,00
Note	**7,33** sur 10,00 (**73,33**%)

Question **1**
Correct
Note de 1,00 sur 1,00

L'acquisition et le déploiement d'un système de détection d'intrusion (IDS) constitue une mesure de bastionnage de réseau (« network hardening »).

Veuillez choisir une réponse.

détecte mais bloque pas l'attaque

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **2**
Correct
Note de 1,00 sur 1,00

Qu'est-ce qu'un faux négatif ?

a. Une alerte générée par un IDS alors qu'il n'y a pas d'attaque
b. Une attaque qui n'est pas détectée par un IDS ✔

Votre réponse est correcte.

La réponse correcte est :
Une attaque qui n'est pas détectée par un IDS

Question **3**
Correct
Note de 1,00 sur 1,00

Lequel de ces comportements malveillant risque le moins de causer une alerte sur un IDS réseau ?

Veuillez choisir une réponse.

voit fichier déplacer entre client et serveur avec signature

client ramène fichier sur son ordi via session ssh IDS ne détecte pas

a. Lecture du fichier /etc/shadow dans une console telnet
b. Édition du fichier de mot passe dans une console SSH ✔
c. Téléchargement d'un virus connu par FTP
d. Exploitation à distance d'un débordement de tampon sur le service mail
e. Attaque d'injection SQL sur un service web

Votre réponse est correcte.

La réponse correcte est : Édition du fichier de mot passe dans une console SSH

Question 4
Correct
Note de 1,00 sur 1,00

Un IDS par signature ne sait pas détecter les attaques de type "zero-day"

Veuillez choisir une réponse.

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question 5
Incorrect
Note de 0,00 sur 1,00

L'utilisation de SSL sur la couche application (couche 7) pour pallier les faiblesses d'un chiffrement WEP sur la couche de lien de donnée (couche 2) est un exemple de défense en profondeur.

profondeur avec par exemple 2 pare-feu

Veuillez choisir une réponse.

- Vrai ✖
- Faux

La réponse correcte est « Faux ».

Question 6
Correct
Note de 1,00 sur 1,00

Dans l'établissement d'une session SSL entre la machine client Alice et le serveur Bob, Alice envoie à Bob sa clé privée afin qu'il puisse l'utiliser pour chiffrer le reste de la session.

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question 7
Correct
Note de 1,00 sur 1,00

Il n'existe pas encore d'alternatives sécurisées qui pourraient remplacer le protocole IP par une version sécurisée qui assureraient la confidentialité et l'intégrité des paquets transmis sur le réseau

IPsec
IPv6 par default IPsec
confidentialité,
intégrité

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

La réponse correcte est « Faux ».

Question 8
Incorrect
Note de 0,00 sur 1,00

Laquelle de ces attaques seraient la plus difficile à détecter par un système de détection d'intrusion basé sur les réseaux (« network IDS » ou « NIDS ») ?

ARP est de la couche 2 data link (lien de données) IDS agit sur couche 3 donc ne le voit pas

Veuillez choisir une réponse.

a. Une attaque d'interception de traffic réseau par empoisonnement du cache ARP (« ARP cache poisoning »).

b. Une attaque de déni de service (DoS) par inondation de requêtes http.

c. Une attaque ciblée où le pirate envoie à la cible un courriel contenant un lien vers un site Web infecté. ✖

d. Une attaque utilisant l'envoi d'un exploit de type « shell code » vers une application réseau vulnérable qui a un port ouvert.

Votre réponse est incorrecte.

La réponse correcte est : Une attaque d'interception de traffic réseau par empoisonnement du cache ARP (« ARP cache poisoning »).

Question 9
Correct
Note de 1,00 sur 1,00

Laquelle de ces affirmations concernant l'attaque "Smurf" est fausse ?

a. C'est une attaque par amplification

b. Pour se protéger contre cette attaque. il suffit de configurer correctement le pare-feu

c. C'est une attaque par inondation contre le protocole ICMP

d. C'est une attaque par inondation contre le protocole TCP ✔

Votre réponse est correcte.

La réponse correcte est :
C'est une attaque par inondation contre le protocole TCP

Question 10
Correct
Note de 1,00 sur 1,00

Les règles de détection d'un détecteur d'intrusion réseau (« network IDS ») n'ont pas besoin d'être mises à jour comme c'est le cas pour celles d'un logiciel anti-virus.

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

Question 11

Question 11
Incorrect
Note de 0,00 sur 1,00

Vous voulez empecher que des attaquants puissent realiser une attaque de balayage de ports (port scan) avec l'outil nmap sur vos serveurs faisant face à l'Internet. Quel serait le moyen le plus efficace de protéger les services (excluant ceux qui doivent rester disponibles, comme le service web sur votre serveur web) ?

Veuillez choisir une réponse.

a. VPN ✖
b. IDS
c. Pare-feu à filtrage de paquets (packet filter firewall)
d. Pare-feu applicatif (Application Layer firewall)

Votre réponse est incorrecte.

La réponse correcte est : Pare-feu applicatif (Application Layer firewall)

Question 12
Correct
Note de 1,00 sur 1,00

Il est possible de faire nativement du chiffrement dans toutes les couches du modèle ISO sauf :

Veuillez choisir une réponse.

a. La couche lien de données (couche 2)
b. La couche application (couche 7) ✔
c. La couche réseau (couche 3)
d. La couche transport (couche 4)

aucun chiffrement sur couche 7

Votre réponse est correcte.

La réponse correcte est : La couche application (couche 7)

Question 13
Correct
Note de 1,00 sur 1,00

Dans l'établissement d'une session SSL les étapes suivantes sont réalisées sauf :

Veuillez choisir une réponse.

a. Le client contacte le serveur en lui demandant d'établir une session sécurisée
b. Le serveur choisi un algorithme cryptographique parmi la liste d'algorithmes proposée par le client
c. Le serveur envoie son certificat de clé publique au client, qui le vérifie
d. Le serveur choisit une clé de session, un algorithme de chiffrement asymétrique ✔

Votre réponse est correcte.

La réponse correcte est : Le serveur choisit une clé de session, un algorithme de chiffrement asymétrique

Question 14
Correct
Note de 1,00

Un réseau privé virtuel (VPN) permet de réduire le risque en termes des facteurs suivant sauf :

Veuillez choisir une réponse.

sur 1,00

a. Confidentialité

b. Intégrité

c. Disponibilité

d. Traçabilité ✔

VPN ne peut pas tracer la source de la connection d'un utilisateur externe

Votre réponse est correcte.

La réponse correcte est : Traçabilité

Question **15**

Incorrect

Note de 0,00 sur 1,00

Laquelle de ces réponses est fausse. L'utilisation d'un petit routeur sans-fils pour accéder à Internet dans un petit bureau ou domicile, et qui utilise le protocole NAT pour donner des adresses privées à ses utilisateurs :

Veuillez choisir une réponse.

a. Empêche un attaquant étant sur Internet de balayer directement le réseau de machines desservies par le routeur

b. N'est pas compatible avec l'utilisation d'un VPN

c. Remplace l'adresse source IP (« src IP ») et le port source IP (« src port ») d'un paquet UDP sortant par l'adresse publique du routeur et un port source du routeur attribué par celui-ci à cette connexion.

d. Peut constituer un risque de sécurité important si la clé cryptographique utilisée pour chiffrer le trafic WIFI n'est pas choisie adéquatement par l'utilisateur. ✖

routeur sans fil
avec NAT compatible avec VPN

Votre réponse est incorrecte.

La réponse correcte est : N'est pas compatible avec l'utilisation d'un VPN

◀ Support-Séance12-Cours Aller à... Support-Séance12-Exercices ▶

Commencé le	mercredi 3 mai 2023, 01:35
État	Terminé
Terminé le	mercredi 3 mai 2023, 01:46
Temps mis	11 min 7 s
Points	9,00/11,00
Note	**8,18** sur 10,00 (**81,82**%)

Question **1**

Correct

Note de 1,00 sur 1,00

Lequel de ces livrables n'est pas normalement le résultat d'une inspection furtive (« penetration testing »)

Veuillez choisir une réponse.

a. Une preuve fumante de pénétration, comme par exemple un fichier électronique très confidentiel.

b. Un rapport énumérant des recommandations sur la gouvernance des processus de gestion de la sécurité informatique. ✔

c. Une liste de vulnérabilités techniques découvertes dans les systèmes informatiques examinés.

d. Un rapport décrivant les méthodes employées pour arriver à pénétrer les systèmes.

Votre réponse est correcte.

La réponse correcte est : Un rapport énumérant des recommandations sur la gouvernance des processus de gestion de la sécurité informatique.

Question **2**

Correct

Note de 1,00 sur 1,00

Le terme "propriétaire de système" (stakeholder en anglais) désigne l'administrateur de système qui a la charge du système informatique en question.

Veuillez choisir une réponse.

Vrai

Faux ✔

La réponse correcte est « Faux ».

Question **3**

Correct

Note de 1,00 sur 1,00

Lequel de ces intervenants est le plus en mesure d'être capable d'évaluer l'impact et d'identifier les acteurs qui pourraient menacer les biens informatiques d'une entreprise

Veuillez choisir une réponse.

Veuillez choisir une réponse.

a. Le gestionnaire responsable (« Stakeholder ») ✔

b. Le responsable de la sécurité des systèmes d'inrformation

c. Le « Chief Information Officer » (CIO) ou directeur du département des technologies d'information

d. Le responsable des ressources humaines

Votre réponse est correcte.

La réponse correcte est : Le gestionnaire responsable (« Stakeholder »)

Question **4**

Incorrect

Note de 0,00 sur 1,00

En sécurité informatique, le devoir premier de l'ingénieur informatique ou l'ingénieur logiciel consiste à :

Veuillez choisir une réponse.

a. S'assurer que les programmes qu'ils développent ont fait l'objet de rigoureuses vérifications et sont libres de bogues pouvant mener à l'existence de vulnérabilités

b. Assurer la confidentialité des vulnérabilités qu'ils pourraient découvrir, afin d'éviter que des pirates informatiques puissent s'en servir à des fins néfastes

c. Assurer la protection du public

d. Minimiser le risque sur les biens informatiques de son client (le « stakeholder ») ✖

Votre réponse est incorrecte.

La réponse correcte est : Assurer la protection du public

Question **5**

Correct

Note de 1,00 sur 1,00

Lors d'un test de pénétration réaliste du réseau d'une grande entreprise de construction (« red teaming »), l'équipe d'audit de sécurité arrive à obtenir une copie de l'appel d'offre secret pour un projet de plusieurs milliards de dollars pour la construction d'un nouveau pont sur le St-Laurent, que la compagnie devait déposer d'ici 12 heures au Ministère des transports. L'équipe d'audit a réussi cet exploit en interceptant le signal du réseau sans-fils au café « Troisième Tasse » en face du siège social de la compagnie. Laquelle de ces réactions par le PDG est la plus appropriée ?

Veuillez choisir une réponse.

a. Interdire aux employés d'aller boire du café à Troisième Tasse et ce, que jusqu'à nouvel ordre.

b. Annuler la participation de la compagnie à l'appel d'offre ou du moins modifier l'appel d'offre.

c. Demander la démission immédiate de son chef de sécurité informatique.

d. Poursuivre l'équipe d'audit en cours et leur imposer un bâillon sur les informations qu'ils ont découvertes.

e. Mettre en place une nouvelle politique de sécurité pour les portables corporatifs, y compris un programme de sensibilisation des usagers. ✔

Votre réponse est correcte.

La réponse correcte est : Mettre en place une nouvelle politique de sécurité pour les portables corporatifs, y

La réponse correcte est : Mettre en place une nouvelle politique de sécurité pour les portables corporatifs, y compris un programme de sensibilisation des usagers.

Question **6**

Correct

Note de 1,00 sur 1,00

La responsabilité professionnelle de l'ingénieur à l'égard du public ne s'applique pas dans le domaine du génie informatique étant donné que l'on n'a pas besoin d'être ingénieur pour œuvrer dans le domaine de l'informatique

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **7**

Correct

Note de 1,00 sur 1,00

Un membre de l'équipe de sécurité a découvert une vulnérabilité non connue dans le logiciel utilisé par une entreprise pour implémenter son site Web et l'a rapidement communiqué aux autres membres de l'équipe. Cette situation constitue un risque informatique

Veuillez choisir une réponse.

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question **8**

Correct

Note de 1,00 sur 1,00

Même si un risque a été identifié dans l'analyse de risque et accepté par le propriétaire du système ("stakeholder"), l'ingénieur est ultimement responsable des incidents de sécurité qui survienne en production

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **9**

Correct

Note de 1,00 sur 1,00

Au Québec, les membres de l'Ordre des ingénieurs du Québec (OIQ) sont les seuls qui peuvent porter légalement le titre d'« ingénieur informatique »

Veuillez choisir une réponse.

- Vrai ✔
- Faux

La réponse correcte est « Vrai ».

Question **10**

Correct

Note de 1,00 sur 1,00

Au Québec, seuls les membres de l'Ordre des ingénieurs du Québec (OIQ) peuvent conduire des audits de sécurité des systèmes informatiques reliés aux infrastructures critiques.

Veuillez choisir une réponse.

- Vrai
- Faux ✔

La réponse correcte est « Faux ».

Question **11**

Incorrect

Note de 0,00 sur 1,00

Quoiqu'il n'y ait pas d'acte réservé en génie informatique ni en génie logiciel, ni au Québec ni au Canada, il y a quand même des avantages à ce que les détenteurs de baccalauréat en génie informatique ou génie logiciel s'inscrive au Tableau de l'Ordre des ingénieurs du Québec (OIQ). Laquelle parmi celles-ci est la raison la plus importante pour une telle personne de s'inscrire à l'Ordre.

Veuillez choisir une réponse.

a. L'OIQ offre de la formation professionnelle continue dans le domaine du génie informatique et génie logiciel ✖

b. Si on n'est pas inscrit à l'OIQ il est essentiellement impossible d'obtenir un poste en informatique.

c. Être membre de l'OIQ permet d'avoir une voix et le droit de vote au sein de l'OIQ afin de changer les choses de « l'intérieur ».

d. Le fait de porter le titre « ingénieur » confère un prestige professionnel très important dans le secteur des technologies de l'information.

Votre réponse est incorrecte.

La réponse correcte est : Le fait de porter le titre « ingénieur » confère un prestige professionnel très important dans le secteur des technologies de l'information.

◀ Support-Cours-Séance13 Aller à... Support-Exercices-Séance13 ▶