

[Tableau de bord](#) / [Mes cours](#) / [INF4420A - Sécurité informatique](#) / Semaine #11 - 30 mars 2023 / [Quiz Cours Sécurité Réseau 1](#)

Commencé le jeudi 27 avril 2023, 18:11

État Terminé

Terminé le jeudi 27 avril 2023, 18:30

Temps mis 19 min 38 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. Reverse proxy ✓
- ☐ b. 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 des paquets mal fragmentés
- ☒ b. A envoyer un paquet dont la taille dépasse la taille maximale autorisée (65535 octets) ✓
- ☐ c. A envoyer un paquet avec tous les flags TCP positionnés à 1
- ☐ d. A envoyer un paquet ayant une adresse IP source égale à l'adresse IP destination

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 pas un principe de bastionnage d'un serveur proxy ?

Veillez choisir une réponse.

- ☐ a. Chaque proxy s'exécute comme un usager non privilégié dans un répertoire privé et sécurisé
- ☐ b. Concevoir chaque module de proxy de façon minimale et sécurisée
- ☐ c. Installer uniquement les services nécessaires pour l'administration réseau
- ☒ d. Bloquer le trafic non chiffré ✓

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.

Veillez 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 :

Veillez 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 connaître 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 chaîne n'est pas une chaîne définie par défaut dans Netfilter ?

Veuillez choisir une réponse.

- ☒ a. TRANSFERT ✓
- ☐ b. INPUT
- ☐ c. OUTPUT
- ☐ d. FORWARD

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 chaîne 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

Incorrect

Note de 0,00
sur 1,00

Sous Netfilter, lorsque la chaîne 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 incorrecte.

La réponse correcte est :

Le pare-feu applique le transfert d'adresse sur l'adresse source du paquet

Question 18

Correct

Note de 1,00
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 correcte.

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](#)[Exercice Cours Sécurité Réseau 1 ▶](#)