Commencé le	dimanche 21 avril 2024, 23:39
État	Terminé
Terminé le	dimanche 21 avril 2024, 23:40
Temps mis	6 s
Points	0,00/15,00
Note	**0,00** sur 10,00 (**0**%)

Question 1

Non répondue

Noté 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.

- Vrai
- Faux

La réponse correcte est « Faux ».

Question 2

Non répondue

Noté 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 incorrecte.

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

Question 3

Non répondue

Noté sur 1,00

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

Veuillez choisir une réponse.

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 incorrecte.

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

Question 4

Non répondue

Noté 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

Non répondue

Noté 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.

Veuillez choisir une réponse.

Vrai

Faux

La réponse correcte est « Faux ».

Question 6

Non répondue

Noté 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

Non répondue

Noté 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

Veuillez choisir une réponse.

- Vrai
- Faux

La réponse correcte est « Faux ».

Question 8

Non répondue

Noté 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 ») ?

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

Non répondue

Noté 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 incorrecte.

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

Question 10

Non répondue

Noté 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

Non répondue

Noté sur 1,00

Vous voulez empêcher que des attaquants puissent réaliser 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

Non répondue

Noté 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)

Votre réponse est incorrecte.

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

Question 13

Non répondue

Noté 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 incorrecte.

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

Question 14

Non répondue

Noté sur 1,00

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

Veuillez choisir une réponse.

a. Confidentialité

b. Intégrité

c. Disponibilité

d. Traçabilité

Votre réponse est incorrecte.

La réponse correcte est : Traçabilité

Question 15

Non répondue

Noté 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.

Votre réponse est incorrecte.

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