| | |
|---|---|
| **Commencé le** | vendredi 30 avril 2021, 09:30 |
| **État** | Terminé |
| **Terminé le** | vendredi 30 avril 2021, 11:29 |
| **Temps mis** | 1 heure 59 min |
| **Points** | 32,00/39,00 |
| **Note** | **32,82** sur 40,00 (**82**%) |

Question **1**

Correct

Note de 1,00 sur 1,00

Dans le modèle "standard" d'une attaque via le réseau, la phase de reconnaissance consiste à :

a. Identifier les caractéristiques techniques de la cible (configuration, logiciels installés, etc.)

b. Reconnaître si la cible trouvée est d'intérêt pour l'attaquant

c. Extraire vers l'extérieur le plus d'information possible des bases de données et fichiers contenu sur la cible

d. Repérer "où" sur le réseau se trouve la ou les cibles des attaques, p.ex. nom de domaine, adresse IP

La réponse correcte est :
Repérer "où" sur le réseau se trouve la ou les cibles des attaques, p.ex. nom de domaine, adresse IP

Question **2**

Incorrect

Note de 0,00 sur 1,00

Laquelle de ces réponses n'est pas une caractéristique de la détection par règle :

a. La détection par règle à le désavantage que si l'attaquant connaît la règle de détection il peut souvent trouver une façon de réaliser son activité de piratage sans déclencher cette règle

b. Il n'est pas nécessaire qu'un humain examine les alertes d'un IDS par règle, car celle-ci sont facilement interprétable par un algorithme automatique de protection des systèmes.

c. La détection par règle n'a pas de période d'"apprentissage" des activités normales du réseau et peut-être déployée immédiatement

d. Il existe un compromis entre taux de faux positif (fausse alertes) et taux de faux négatif (alertes manquées), souvent déterminé par le seuil de détection ✖

Question **3**

Correct

Note de 1,00 sur 1,00

Laquelle de ces réponses n'est pas un type d'attaque de déni de service :

a. Attaque de déni de service distribuée (Distributed DoS)

b. Attaque par exploitation d'une porte dérobée (Backdoor DoS)

c. Attaque par inondation HTTP (HTTP Flooding)

d. Attaque par vulnérabilité (Crippling DoS)

Question **4**

Incorrect

Note de 0,00 sur 1,00

L'utilisation de requêtes SQL pré-enregistrées (SQL stored procedures) dans un moteur de base de données constitue une bonne contre-mesure contre les attaques informatiques sur des applications Web pour toutes ces raisons sauf

a. La requête SQL est précompilée par le moteur de base de données ce qui permet qu'elle soit exécutée plus rapidement qu'une requête SQL transmise par le réseau, qui elle est interprétée et exécutée en temps réél

b. L'utiilsation de stored procedures permet de restreindre l'utilisation de SQL à seulement les requêtes qui sont nécessaires pour la bonne exécution de l'application Web

c. Des permissions peuvent être attribuées à niveau de la stored procedure correspondant à des groupe d'usagers restreints ✖

d. Parce que le code SQL des stored procedure est prédéterminé d'avance, du code SQL contenu dans des chaînes de caractère passées en paramètres au stored procedure ne serait pas interprété comme du code SQL, juste comme une chaîne de caractère.

Question **5**

Correct

Note de 1,00 sur 1,00

Par rapport aux caractéristiques et fonctionnalités d'un réseau privé virtuel (VPN) utilisant le protocole IPSEC, laquelle de ces réponses est fausse :

a. Établit un concept de "session" permettant d'éviter la transmission des paramètres cryptographiques à chaque paquet

b. Permet de chiffrer le trafic IP entre deux correspondants à travers l'Internet

c. Permet d'assurer l'intégrité des paquet IP transmis entre correspondant du même réseau virtuel

d. 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 **6**

Incorrect

Note de 0,00 sur 1,00

Laquelle des réponses suivantes n'est pas une contre-mesure efficace contre les attaques par débordement de tampon sur la pile.

a. Utiliser des langages de programmation plus modernes tel que le Javascript

b. Configurer le système d'exploitation pour que l'espace mémoire alloué soit attribué aléatoirement (ASLR)

c. Programmer de façon à éviter de passer des pointeurs de tampon en paramètre sans passer aussi l'information de la quantité de mémoire qui y a été allouée

d. Déployer une solution de protection des pointeurs de retour du type canari (tel que Stack Guard)

Question **7**

Correct

Note de 1,00 sur 1,00

La sécurité des protocoles SSL et TLS repose sur la fiabilité de l'infrastructure à clé publique (ICP) déployée pour assurer l'authenticité des certificats de clé publique envoyé par les serveurs Web lors de l'établissement d'une connexion SSL/TLS. Un des problèmes de cette ICP est le fait qu'elle est hiérarchique et qu'elle repose sur la fiabilité des plusieurs autorité de certification racine (root CA) présentement supportés par l'ensemble des fureteurs Web présentement utilisés par la majorité des usagers. Laquelle de ces réponses n'est pas une raison (ou est la raison la plus faible) pour mettre en doute la fiabilité de ces autorités racine et donc questionner la sécurité de SSL/TLS.

a. Certaines autorités racines signent les certificats avec des algorithmes de clé publique qui ne sont même pas résistants à des attaques de cryptanalyse quantique

b. Le processus de vérification de l'identité des personnes et de la propriété d'un domaine par la personne ou organisation qui demande un certificat n'est pas standard et varie d'une autorité racine à l'autre

c. Il y a très peu d'informations disponibles sur certaines de ces autorités racines, ce qui rend difficile de vérifier quels sont les intérêts (commerciaux ou autres) qui sont derrière ces autorités racines.

d. Certaines des autorités racines sont de petites organisations à but non lucratif qui pourraient être vulnérables à des attaques informatiques ciblées dont le but serait de voler les clés privées utilisés pour la signature de certificat.

Question **8**

Correct

Note de 1,00 sur 1,00

Concernant les attaques de Cross-Site Scripting (XSS) contre des serveurs Web, laquelle de ces affirmations est vraie:

a. Elles permettent de prendre le contrôle ("owner") le serveur Web qui démontre ce type de vulnérabilité

b. Elle permette de relayer le client (fureteur) sur un site malveillant avec les mêmes privilèges que s'il était sur le site qui a la vulnérabilité

c. Ne sont pas possible si le site ciblé utilise le protocole SSL ou TLS pour protéger la session HTTP

d. Sont en général possible grâce à la présence d'une vulnérabilité de type débordement de tampon sur le tas dans l'application We

Question **9**

Correct

Note de 1,00 sur 1,00

Laquelle des raisons mentionnées n'est pas une bonne réponse en ce qui concerne la difficulté de créer du "shell code" qui puisse être utilisé dans une attaque par débordement de tampon sur une application vulnérable :

a. 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

b. 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

c. La distance entre le début du tampon et le pointeur de retour n'est pas toujours la même car l'executiion du programme n'est pas déterministe

d. Il faut absolument éviter que le shell code contiennent des caractères NULL (0x00) qui pourraient facilement être détectés par des IDS ou autre type d'outils de sécurité informatique

Question **10**

Correct

Note de 1,00 sur 1,00

Lequel de ce type de vulnérabilité logiciel ne peut pas être adresser en utilisant des techniques vérification et validation des entrées d'un programme

a. Débordement de tampon sur la pile

b. SQL Injection

c. Cross-site Scripting (XSS)

d. Erreur de logique d'application

Question **11**

Correct

Note de 1,00 sur 1,00

Concernant l'utilisation des secure token dans les applications Web, laquelle de ces affirmations est fausse

a. L'utilisation de secure token est un moyen de protection contre le Cross Site Request Forgery (XSRF)

b. Un "secure token" est la même chose qu'un "session ID"

c. La valeur d'un secure token est choisie et vérifiée par le serveur en correspondance avec le session ID

d. Sur le fureteur du client, le secure token est éphémère est n'est pas stocké dans la base de données de cookies

Question **12**

Correct

Note de 1,00 sur 1,00

Laquelle de ces réponses ne constitue pas une attaque rendue possible par une vulnérabilité logiciel :

a. Attaque cryptanalytique utilisant une faiblesse d'un l'algorithme de chiffrement obsolète utilisé dans le logiciel

b. Vulnérabilité de la chaîne de format (format string vulnerability)

c. Attaque de déni de service de type "crippling DoS"

d. Débordement de tampon sur le tas (heap buffer overflow)

Question **13**

Correct

Note de 1,00 sur 1,00

Le contrôle d'accès aux biens informatiques inclut les aspects suivants sauf

a. Identification ("Identification")

b. Autorisation ("Authorization")

c. Disponibilité ("Availability")

d. Authentification ("Authentication")

Question **14**

Correct

Note de 1,00 sur 1,00

Laquelle de ces informations est fausse par rapport au contrôle d'accès discrétionnaire (Discretaionnary Access Control ou DAC)

a. Les usagers peuvent changer les permissions des fichiers qui leur appartiennent

b. Est plus permissif que le modèle de contrôle d'accès obligatoire (Mandatory Access Control ou MAC)

c. C'est le modèle de contrôle d'accès utilisé pour les fichiers par les systèmes d'exploitation Linux et Windows

d. Implémente la règle "no write down" qui empêche un programme d'écrire dans un fichier pour lesquels il n'a pas le bon niveau d'accès

Question **15**

Correct

Note de 1,00 sur 1,00

Laquelle de ces propriétés de sécurité ou caractéristiques ne fait pas partie du modèle Bell et La Padula sous-jacent au contrôle d'accès obligatoire (Mandatory Access Control ou MAC)

a. No Write Down

b. Étiquetage des données en fonction de leur niveau de confidentialité ("classification")

c. Domain Type Enforcement (DTE)

d. No Read Up

Question **16**

Correct

Note de 1,00 sur 1,00

Laquelle de ces informations sur le contrôle d'accès basé sur les rôles (Role-based Access Control ou RBAC) est fausse

a. La philosophie AGLP (Access, Global, Local, Permissions) est un exemple d'application de la méthode RBAC

b. Ce modèle essaie de minimiser la complexité de la gestion des accès des usagers indviduels

c. Un sujet ne peut pas jouer plusieurs rôles dans la même session

d. Le modèle RBAC associe les droits d'accès à une notion de session car le même usager ne joue pas toujours le même rôle

Question **17**

Correct

Note de 1,00 sur 1,00

La contrainte RBAC qui empêche que le même usager puisse remplir deux rôles précis dans la même session s'appelle:

a. Single Role Access Control Policy

b. Une telle contrainte n'existe pas dans RBAC: un utilisateur peut toujours remplir deux rôles ou plus dans la même session

c. No write down

d. Separation of Duty

Question **18**

Correct

Note de 1,00 sur 1,00

Laquelle des réponses suivantes n'est pas une propriété ou objectif de la signature numérique

a. Authenticité du message

b. Non répudiation

c. Confidentialité du message

d. Intégrité du message

Question **19**

Correct

Note de 1,00 sur 1,00

Laquelle de ces réponses n'est pas un objectif ou un principe de la gestion des identités et des accès (GIA, ou Identity Access Management - IAM en anglais)

a. La séparation entre les fonctions de contrôle d'accès (authentification et autorisation) et les fonctions du système (logique d'application, règles d'affaires, etc.)

b. Assurer une gestion intégrée et centraliser des paramètres d'authentification et des permissions d'accès

c. Provisionnement de solution intégrée d'authentification avec l'utilisation de solution de Single Sign On (SSO)

d. La comparaison continue entre les accès attribués dans le système d'IAM et les politiques de sécurité

Question **20**

Correct

Note de 1,00 sur 1,00

Laquelle de ces méthodes ne constitue pas un exemple de facteur d'authentification de quelque chose qu'on possède (jeton d'authentification)

a. Une carte à puce sans contact utilisée pour autoriser une transaction bancaire

b. Une clé de métal utilisé dans une serrure qui permet le démarrage d'un ordinateur de bureau

c. Un téléphone portable intelligent utilisé pour prendre une photo du visage de l'usager, qui est envoyé à un serveur par Internet pour authentifier l'usager

d. Un téléphone portable intelligent utilisé pour générer un mot de passe à usage unique

Question **21**

Correct

Note de 1,00 sur 1,00

Un des principaux avantages de l'utilisation de la cryptographie a courbe elliptique (Elliptic Curve Cryptography ou ECC) est

a. qu'elle est plus résistante aux attaques de cryptanalyse post-quantique

b. que son utilisation est gratuite car elle ne repose pas sur des brevets commerciaux

c. qu'elle peut être rendue très performante grâce à l'utilisation de GPU pour calculer les points sur des courbes elliptiques en 3D

d. est le fait que pour un niveau de sécurité équivalent la taille des clés est plus petite, ce qui rend les signatures plus petites également, ce qui est attractif dans des applications où la bande passante est réduite

Question **22**

Correct

Note de 1,00 sur 1,00

Laquelle de ces affirmation sur l'utilisation de solutions de gestion centralisé de mots de passe (Singe Sign On ou SSO) est fausse

a. A comme désavantage de constituer un point de défaillance unique

b. La base de données de mots de passe doit être protéger par un mot de passe "maître" qui les protège tous

c. Protège contre les compromissions de données d'authentification (p.ex. /etc/shadow) dans les serveurs d'authentification

d. Elle a l'avantage de permettre à l'utilisateur de choisir des mots de passe de plus haute entropie

Question **23**

Correct

Note de 1,00 sur 1,00

Malgré que plusieurs experts (y compris le président Obama) aient annoncée la mort imminente du mot de passe, les nouvelles de sa mort semble avoir été grandement exagérée. Laquelle de ces raisons n'est pas une des raisons de son succès passé et présent.

a. Son utilisation ne nécessite d'aucun matériel (hardware) supplémentaire et a donc un coût supplémentaire négligeable

b. Si le mot de passe d'un usager est compromis, il est relativement facile pour celui-ci de le ré-initialiser, ce qui permet de réduire l'impact d'une telle situation

c. C'est un des rares facteurs d'authentification qui puisse être utilisé facilement à travers un réseau informatique

d. L'authentification par mot de passe n'est pas vulnérable aux attaques de rejeu

Question **24**

Incorrect

Note de 0,00 sur 1,00

Par rapport à la cryptographie post-quantique laquelle de ces affirmations est vraie

a. La plupart des algorithmes de cryptographie post-quantique ont une performance similaire à celle des algorithmes cryptographiques équivalent actuels

b. Ce terme désigne les algorithmes de cryptographie à clé symétrique pour lesquels aucun algorithme de cryptanalyse quantique efficace est connu

c. Il existe déjà plusieurs algorithmes de cryptographie post-quantique qui ont étés sélectionnés et évalués par des institutions de normes et standardisation

d. Constitue une préoccupation essentiellement "académique" et peu urgente car aucun ordinateur quantique suffisamment grand n'a été construit pour implémenter les algorithmes de cryptanalyse quantique

Question **25**

Terminer

Non noté

Laquelle de ces affirmation sur l'authentification par défi-réponse (Challenge-response) est vraie

a. N'est utilisé que pour des applications Web

b. Ne nécessite pas que le défi (challenge) soit choisie avec un haute entropie

c. Ne permet pas que le serveur Bob puisse authentifier le client Alice

d. Ne protège pas contre les attaques par rejeu

Question **26**

Correct

Note de 1,00 sur 1,00

L'entropie fait partie de la réponse à toutes ces questions sauf

a. La difficulté de factoriser des grands entiers afin de retrouver des clés privées dans certains algorithmes à clé publique

b. La difficulté de conduire une attaque par force brute sur un système d'authentification par mot de passe

c. L'utilisation adéquate d'un codage en terme résistance à des efforts cryptanalytiques par texte clair choisi

d. L'efficacité des algorithmes de compression

Question **27**

Correct

Note de 1,00 sur 1,00

Laquelle de ces méthodes n'est pas adéquate pour assurer l'authenticité d'un message envoyé par Alice à Bob dans un contexte ou Ève peut intercepter et modifier le message envoyé d'Alice à Bob de façon imperceptible.

a. Utilisation de signature numérique par Alice pour signer le message avant de le transmettre à Bob avec le certificat de clé publique d'Alice

b. Utiliser une fonction de hachage pour calculer le haché du message qui est transmis par Alice à Bob en utilisant un canal altern

c. Utiliser le protocole HMAC en s'assurant qu'Alice et Bob aient préalablement échanger un secret partagé S

d. Utilisation du protocole d'échange de clés de Diffie-Hellman pour échanger une clé secrète qui peut être utiliser pour le protocole HMAC

Question **28**

Correct

Note de 1,00 sur 1,00

Laquelle de ces affirmation est vraie concernant la cryptographie quantique

a. Est une construction théorique pour laquelle aucune démonstration expérimentale ni solution disponible commercialement exist

b. Ce terme désigne les algorithmes de cryptographie qui sont résistants aux attaques de cryptanalyse quantique

c. A été récemment découverte par des chercheurs en Chine

d. Ce terme désigne des algorithmes de cryptographie qui se basent sur les propriétés de la physique quantique pour assurer leur sécurité

Question **29**

Correct

Note de 1,00 sur 1,00

Plusieurs annoncent depuis plusieurs années la mort imminente du mot de passe comme mécanisme d'authentification sur les systèmes informatiques (y compris même le président américain Barak Obama!). Laquelle de ces caractéristiques constitue la raison principale pour laquelle le mot de passe est "mort".

a. La sécurité de l'authentification par mot de passe peut être compromise par la capture des bases de données de hachés de mots de passe

b. L'authentification par mot de passe est vulnérable à des attaques par logiciel malveillant tel que des enregistreurs de touches (keylogger)

c. Aujourd'hui, les mots de passe utilisés pour l'authentification dans les applications Web peuvent facilement être capturés par un Ève qui peut intercepter les paquets IP transmis entre le fureteur d'Alice et le serveur Web de Bob.

d. Il est peu naturel (et donc peu fréquent) pour les usagers de choisir des mots de passe avec haute entropie et qui soient en même temps facile à retenir

Question **30**

Correct

Note de 1,00 sur 1,00

En cryptographie le principe de souveraineté de clé (choisissez la bonne réponse)

a. Dit que les clés cryptographiques devraient être générées par la personne ou l'autorité à qui cette clé appartient et qui va l'utiliser

b. Qu'un état souverain devrait avoir la capacité d'intercepter des communications protégées par une clé cryptographique s'il a une raison légitime pour le faire (p.ex. mandat judiciaire d'écoute, sécurité nationale, etc.)

c. Consiste à s'assurer qu'une clé cryptographique symétrique ne puisse être partagée que par des individus ayant le même niveau d'accès, et en particulier citoyen d'un même pays

d. Implique qu'une clé cryptographique ne devrait servir qu'à un seul usage (p.ex. signer ou chiffrer, mais pas les deux)

Question **31**

Correct

Note de 1,00 sur 1,00

Laquelle de ces informations est fausse concernant l'algorithme cryptographique du masque jetable

a. Permet une sécurité parfaite en autant que la taille de la clé soit aussi grande que celle du message et qu'elle soit choisie avec une entropie maximale

b. Est résistant à la cryptanalyse quantique

c. N'est pas performant car elle demande des temps de calcul considérablea, même pour des fichiers de taille moyenne (quelques MB)

d. Aurait été utilisé par le Che Guevara pour transmettre ou recevoir des informations chiffrées envoyées à La Havane lorsqu'il menait des opérations de guerrilla en Bolivie peu avant sa mort.

Question **32**

Correct

Note de 1,00 sur 1,00

Qu'est-ce qui est vrai concernant l'utilisation de techniques de correction d'erreur ?

a. La correction d'erreur à partir du syndrome doit être fait avant le déchiffrement du message

b. Elle permet de protéger l'intégrité du contenu du message contre un attaquant malveillant

c. Le calcul et l'ajout du syndrome doit être fait le plus tôt possible, soit à la couche la plus haute du modèle ISO (idéalement couche application)

d. Son lien avec l'entropie du message est décrit par le 1er théorème de Shannon

Question **33**

Terminer

Note de 2,00 sur 2,00

Qu'est-ce qui est vrai concernant l'utilisation de techniques de correction d'erreur ?

Expliquez votre choix de réponse à la question antérieure.

Le lien avec l'entropie du message est décrit par le 2ième théorème de Shannon. Le chiffrement et déchiffrement ne corrige pas les erreurs et il faut donc appliquer le syndrome après le chiffrement et avant le déchiffrement puisqu'une erreur introduite entre le chiffrement et le déchiffrement pourrait donner un tout autre message considérant la propriété de diffusion recherché par les algorithmes de chiffrement.

Question **34**

Correct

Note de 1,00 sur 1,00

Lequel de ces services doit absolument être placé dans la DMZ

a. Serveur de base de données utilisée par une application Web externe

b. Proxy web applicatif protégeant les connexions sortantes

c. Serveur mail IMAP et POP3 permettant aux usagers d'accéder à leurs boites au lettre

d. Serveur Web pour usager externe

Question **35**

Terminer

Note de 2,00 sur 2,00

Lequel de ces services doit absolument être placé dans la DMZ

Explique votre réponse à la question précédente

Les serveurs mail ne seront définitivement pas dans la DMZ puisqu'ils sont pour usage interne.

Le serveur Web pour usager externe pourrait se retrouver dans la DMZ, mais l'utilisation d'un proxy web entre l'extérieur et le serveur web rend cela non-nécessaire.

Le serveur de base de données utilisée par une application Web externe communique aussi à travers le proxy web et ne sera donc pas dans la DMZ.

Au final, seul le proxy web doit être dans la DMZ puisque c'est celui-ci qui agit en tant que pont entre l'extérieur et l'intérieur rendant de la sorte tous les autres serveurs indirectement connecté à l'extérieur. Ils n'ont donc plus le besoin d'être dans la DMZ.

Question **36**

Incorrect

Note de 0,00 sur 1,00

Laquelle de ces méthodes est la moins sécuritaire pour assurer l'authentification des usagers externes sur une application Web

a. Faire la vérification du nom d'usager et mot de passe par du code client (sur le fureteur) écrit dans un langage sécuritaire comm le Java

b. Stocker les noms d'usager et les mots de passe en clair dans le moteur de base de données utilisé par l'application Web, et faire la vérification du mot de passe à niveau du serveur Web

c. Envoyer le nom d'usager et le mot de passe vers un serveur d'authentification externe qui fait la vérification

d. Faire une vérification sur le serveur Web en utilisant le fichier /etc/passwd et/ou le fichier /etc/shadow sur ce serveur

Question **37**

Terminer

Note de 0,00 sur 2,00

Laquelle de ces méthodes est la moins sécuritaire pour assurer l'authentification des usagers externes sur une application Web.

Expliquez votre réponse à la question précédente

L'envoi vers un serveur externe implique qu'il faut compromettre les deux serveurs et c'est donc plus difficile.

Dans le cas de la vérification sur le serveur, le mot de passe est haché nécessitant de déchiffrer celui-ci.

La vérification sur le fureteur peut impliquer certains dangers puisque l'utilisateur pourrait compromettre le code d'une certaine manière afin de permettre la connexion.

Cependant, le plus dangereux reste le stockage des noms d'usagers et mots de passe en clair puisqu'il suffit que le serveur web soit corrompu ou qu'il possède une faille logique afin qu'un attaquant récupère toutes les noms d'usagers et mots de passes des utilisateurs permettant ainsi d'avoir tous les accès.

◄ Annonces

Aller à...