Evaluation Finale

Partie 1 :

Une coopérative a mis en place un site de vente de ses produits en ligne (e-commerce).
Cette coopérative a un chiffre d'affaire annuelle de 10 Millions Dhs.
Le site de cette coopérative subit des attaques DoS de temps en temps.
Chaque attaque correspond à une perte de 5% du chiffre d'affaire annuel.
Les statistiques ont montré qu'en moyenne, cette coopérative subit 2 attaques/an.
Une protection envisagée par cette coopérative est de prendre le service de protection cloud « CloudFlare » qui coute 50 000Dh/Mois.

Faites une analyse coût/bénéfice concernant cette protection en précisant :

1-Les paramètres :

Asset Value (AV) =

Annual cost of the safeguard (ACS) =

2-Les paramètres avant protection :

Exposure Factor (EF) =

Single loss expectancy (SLE) =

Annualized rate of occurrence (ARO) =

Annualized loss expectancy (ALE) =

3-Les paramètres après protection :

Exposure Factor (EF) =

Single loss expectancy (SLE) =

Annualized rate of occurrence (ARO) =

Annualized loss expectancy (ALE) =

4-Bénifice =

5-Faut-il implémenter cette protection (Oui/Non) et pourquoi ?

Partie 2 :

1-Quel est la finalité de la « Reduction Analysis » ? :

A. une meilleure compréhension de la logique de fonctionnement d'un produit
B. La subdivision de système
C. La réduction du risque
D. L'identification des attaquants

2-Quel est le principe CIA qui signifie que les sujet ont un accès permanant et interrompu aux objets :

A. Identification
B. Disponibilité
C. Cryptage
D. Confidentialité

3-Parmi les suivants quel est celui qui défini les buts et objectifs primaires de la sécurité?

A. Le Périmètre Réseau
B. La Triade CIA
C. Un système autonome
D. Internet

4-Qu'est ce qui est faux ? :
A. La violation de la confidentialité inclue le facteur humain
B. La violation de la confidentialité inclue la gestion de la supervision/surveillance (oversight)
C. La violation de la confidentialité est limitée aux attaques intentionnelles
D. La violation de la confidentialité peut être liée à l'absence de cryptage lors de la transmission de données

5-Qu'est ce qui définie au mieux la méthode STRIDE ? :
A. Méthode de Calcul de Risque
B. Schéma de Classification des Menaces
C. Référentiel Sécurité
D. Standard d'Authentification

6-La méthode DREAD est utilisée pour :

A. Classifier et évaluer les menaces
B. Classifier les attaquants
C. Classifier les attaques
D. Classifier les failles

7- Quand une protection est évaluée, quelles sont les règles suivies ?

A. Le coût annuel des pertes relatives à l'Asset ne doit pas dépasser le coût annuel de la protection.
B. Le coût annuel de la protection doit être égal à la valeur de l'Asset.
C. Le coût annuel de la protection ne doit pas dépasser le coût annuel des pertes relatives à l'Asset.
D. Le coût annuel de la protection ne doit pas dépasser 20% du budget annuel alloué à la sécurité.

8- Vous effectuez une analyse quantitative du risque sur une relation menace/vulnérabilité/risque. Vous sélectionnez une protection. Quand vous faites le calcul lui correspondant, quel est la paramètre qui va changer ?

A. Facteur d'Exposition.
B. Perte individuelle prévue.
C. Valeur de l'Asset.
D. Fréquence annuelle de réalisation.

9- Lequel des éléments suivants n'est pas un élément du processus d'analyse des risques?

A. Analyser les risques pour l'environnement.
B. Création d'un rapport coût / bénéfice pour les protections à présenter décideurs.
C. Choix des protections appropriées et leurs mises en œuvre
D. Evaluation pour chaque menace, la probabilité de sa réalisation et coût des dommages résultants.

10- Quel est le contrôle de sécurité qui a pour but d'empêcher les complicités?

A. Principe du moindre privilège
B. Séparation des tâches
C. Analyse de Risque Quantitative
D. Description des tâches

11- Pour le risque Tsunami Qu'est ce qui n'est considéré comme transfert de risque pour un Datacenter?

A. Installer des digues autour du Datacenter
B. Déplacer le Datacenter d'une localisation côtière loin de la côte
C. Prendre une police d'assurance

12. Quel est la fonction de Serveur d'Accès Réseau dans une architecture RADIUS ?

A. Serveur d'Authentification
B. Client
C. Serveur AAA
D. Firewall

13. Que doit faire une organisation pour détecter les faiblesses ?

A. Valorisation des Assets
B. Modélisation des menaces
C. Analyse des vulnérabilités
D. Evaluation de l'accès

14. Qu'est ce qui est vrai par rapport au Sujet?

A. Un Sujet est toujours un compte utilisateur.
B. Le Sujet c'est toujours l'entité qui fournis ou héberge les données.
C. Le Sujet est toujours l'entité qui reçoit les information ou les données de la part d'un Objet.
D. Une entité ne peut jamais changer de rôle entre Sujet et Objet.

15. Qui alloue les permissions aux utilisateurs dans le modèle discretionary access control ?

A. Administrateurs
B. Access control list
C. Labels assignés
D. La propriétaire des donnés.

16. Une autorité centrale détermine quel fichier l'utilisateur peut accéder. Quelle est la meilleure description ?

A. Une access control list (ACL)
B. Une access control matrix
C. Discretionary access control model
D. Nondiscretionary access control model

17. Une autorité centrale détermine quel fichier l'utilisateur peut accéder en se basant sur la hierarchy de l'organisation. Quelle est la meilleure description ?

A. Discretionary access control model
B. Une access control list (ACL)
C. Rule-based access control model
D. Role-based access control model

18. Quel type de contrôle d'accès utilise des mécanismes software ou hardware pour gérer l'accès aux ressources et systèmes et leur fournit la protection nécessaire ?

A. Administrative
B. Logique/Technique
C. Physique
D. Préventive

19. Un utilisateur se connecte avec un login ID et mot de passe. Quel est le rôle du login ID?

A. Authentification
B. Autorisation
C. Accountability
D. Identification

20. Quel est le paramètre qui empêche les utilisateurs de faire tourner 2 mots de passe ?

A. Complexité
B. Historique
C. Age maximum
D. Longueur

21. Parmi les suivants qui est un exemple d'un facteur d'authentification de Type 2?

A. Quel que chose que vous avez
B. Quel que chose que vous êtes
C. Quel que chose que vous faites
D. Quel que chose que vous connaissez

22. Quelle est l'indication fournie par le crossover error rate (CER) concernant un périphérique biométrique ?

A. La sensibilité est trop élevée.
B. La sensibilité est trop basse.
C. Le point ou les taux des faux rejets et des fausses acceptations sont égaux.
D. Lorsqu'il est élevé il signifie que le périphérique biométrique est très précis.

23. Quel type de contrôle d'accès est basé sur l'utilisation des labels ?

A. Discrétionnaire
B. Non discrétionnaire
C. Obligatoire
D. Basé sur les rôles

24. Parmi ce qui suit sui décrit le mieux les caractéristiques du modèle mandatory access control

A. Utilise le principe explicit-deny
B. Permissive
C. Basé sur les règles
D. Prohibitive

25. Parmi les suivants qui permet de diminuer le succès d'une attaque brute-force on line ?

A. Table Rainbow
B. Verrouillage des comptes
C. Passes avec Salt
D. Cryptage des mots de passe

Répondez aux questions 26 et 27 en se référant au scénario suivant :

Un administrateur a travaillé pour une organisation pendant 10 ans. Il est passé par plusieurs départements IT de l'organisation tout en gardant les différents privilèges qu'il avait lors de son passage dans ces différentes divisions.
Dernièrement les responsables de l'organisation ont découvert qu'il avait effectué des changements non autorisés au système qui ont causé des mal fonctionnements.
Les décideurs ont décidé de le licencier. Il est revenu le lendemain au travail pour récupérer ses affaires et pendant ce temps il a installé un code malicieux programmé à s'exécuter en tant que bombe logique le premier du mois suivant. Ce code a pour objectif de changer les mots de passe administrateurs, d'effacer les fichiers et éteindre 100 serveurs du data center.

26. Quel est le principe qui a été violé pendant la période ou cette personne a été employée de l'organisation ?

A. Implicit deny
B. Perte de disponibilité
C. Défensive privilège
D. Moindre privilège

27. Qu'est ce qui aura permit de découvrir le problème avec ce compte d'utilisateur pendant qu'il était employé par l'organisation ?

A. Politique de forte authentification
B. Authentification multi facteurs
C. Logging
D. Evaluation des comptes

28. Quel est l'objectif primaire de Kerberos?

A. Confidentialité
B. Intégrité
C. Authentification
D. Accountability

29. Quel est le meilleur choix pour supporter un système de gestion d'identité fédérée ?

A. Kerberos
B. Hypertext Markup Language (HTML)
C. Extensible Markup Language (XML)
D. Security Assertion Markup Language (SAML)

30. Quelle est la meilleure description du modèle rule-based access control (rule-BAC) ?

A. Il utilise des règles locales appliquées aux utilisateurs de manière individuelle.
B. Il utilise des règles globales appliquées aux utilisateurs de manière individuelle.
C. Il utilise des règles locales appliquées aux utilisateurs de manière égale.
D. Il utilise des règles globales appliquées aux utilisateurs de manière égale.

31. Quelle est la méthode qui permet aux utilisateurs de s'authentifier une seule fois et accéder aux ressources de plusieurs organisations sans avoir besoin de s'authentifier encore.

32. Citez les 3 tâches principales relatives à la gestion des comptes, de l'accès et de l'accountability durant la vie du compte :

-
-
-

33. Quelle est le nombre de Clés possible pour un espace de Clés à 8 bits?

A. 16
B. 32
C. 128
D. 256

34. John a reçu un email de la part de Bill. Quel service cryptographique doit être assuré pour convaincre John que c'est bien Bill qui est l'expéditeur du message ?

A. Confidentialité
B. Non répudiation
C. Disponibilité
D. Intégrité

35. Quel est le mode opératoire DES utilisé pour les grands messages et qui assure qu'une erreur sur le process cryptage/décryptage n'impactera pas le reste de la communication ?

A. Cipher Block Chaining (CBC)
B. Electronic Codebook (ECB)
C. Cipher Feedback (CFB)
D. Output Feedback (OFB)

36. Quel le nombre de Clés nécessaires pour implémenter une complète communication cryptée de manière symétrique entre 11 participants ?

A. 11
B. 22
C. 55
D. 111

37. Quel le nombre de Clés nécessaires pour implémenter une complète communication cryptée de manière asymétrique entre 20 participants ?

A. 20
B. 40
C. 190
D. 400

38. Si un message qui a une taille de 2048 bits est crypté avec le crypto système El Gamal, quelle sera la taille du message crypté?

A. 1,024 bits
B. 2,048 bits
C. 4,096 bits
D. 8,192 bits

39. Quel est la technique de cryptage que WPA utilise pour protéger les communications sans fil ?

A. TKIP
B. DES
C. 3DES
D. AES

40. Rachid reçoit un message crypté de la part de Samira. Quelle clé il doit utiliser pour décrypter le message ?

A. Clé publique de Rachid
B. Clé privée de Rachid
C. Clé publique de Samira
D. Clé privée de Samira

41. Rachid veut signer numériquement un message qu'il veut envoyer à Samira. Quel clé il doit utiliser pour crypter le message digest ?

A. Clé publique de Rachid
B. Clé privée de Rachid
C. Clé publique de Samira
D. Clé privée de Samira

42. Quel le standard de l'International Telecommunications Union (ITU) qui gouverne la création et la gestion des certificats numériques pour les communications électroniques ?

A. X.500
B. X.509
C. X.900
D. X.905

43. Quel est le port TCP/IP utilisé pour TLS ?

A. 80
B. 220
C. 443
D. 559

44. Quel est l'outil utilisé pour augmenter l'efficacité d'une attaque contre les mots de passe de type brute force ?

A. Rainbow tables
B. Hierarchical screening
C. TKIP
D. Random enhancement

45. Quel est le type de lien qui doit être protégé par un cryptage WPA ?

A. Firewall vers firewall
B. Routeur vers firewall
C. Client vers point d'accès sans fil
D. Point d'accès sans fil vers router