OFPPT	مكتب التكوين المهني وإنعاش الشغل Office de la Formation Professionnelle et de la Promotion du Travail

Examen De Fin De Module

AU TITRE DE L'ANNEE : 2012/2013

Filière : TRI — **Année de formation : 2 A**

Niveau : TS — **Epreuve : théorique**

N°du module : M22 — **Durée : 2h**

Intitulé du module : Notions de sécurité des réseaux informatiques — **VARIANTE : 2**

Date d'évaluation : — **Barème/40**

Exercice 1

Parmi les personnes suivantes, quelles sont celles qui ne devraient pas participer à la modélisation des menaces d'un site Web ? Sélectionnez toutes les réponses qui conviennent.

A. Le développeur qui a écrit l'application du site Web personnalisé et les liens de connexion avec la base de données.

B. L'architecte réseau principal habitué à exécuter des tests de pénétration de réseau.

C. Un technicien en micro-informatique récemment embauché, possédant peu d'expérience informatique et aucune compétence en matière de programmation.

Exercice 2

Parmi les situations suivantes, lesquelles constituent une menace courante à la sécurité physique ? Sélectionnez toutes les réponses qui conviennent.

A. Une porte non verrouillée menant à une salle de serveur.

B. Les faux sols et plafonds d'un centre de données.

C. Les fenêtres donnant sur l'extérieur d'une salle de conférence.

Un ordinateur portable placé sur le siège avant du véhicule verrouillé d'un employé.

Exercice 3

Le directeur des ressources humain d'un entreprise a élaboré une note de service sous forme d'un fichier Microsoft Excel « tabService.xsl » et ce fichier sera partagé pour l'ensemble du personnel dans son poste du travail , Le directeur veut assurer l'intégrité de ce fichier sachant que la politique de sécurité de l'entreprise interdit l'utilisation du messagerie pour la communication entres les utilisateurs. En tant qu'administrateur de sécurité quelle sont les étapes que vous devriez mettre en place pour répondre à ce besoin ?

Exercice 4

Associez chaque menace à l'élément approprié de la classification STRIDE :
Information disclosure (divulgation d'informations)
Denial of service (refus de service)
Elevtion of privilege (élévation de privilège)

Menace	**Classification STRIDE**
Mot de passe envoyé en texte brut à partir d'un ordinateur client vers une base de données	
Un site Web au codage imparfait permet une attaque au niveau du script de tout le site	
L'intrus peut accéder physiquement aux serveurs	
Les mises à jour de la sécurité évitant les saturations de la mémoire tampon ne sont pas appliquées aux serveurs	

Exercice 5

Une autre attaque classique de Déni de Service est l'attaque SYN. Dans une attaque SYN, un attaquant envoie à une victime un flot de paquets SYN avec des adresses sources usurpées (spoofées). La victime initialise des états de connexion et essaie de répondre aux adresses usurpées. Si suffisamment de paquets SYN sont envoyés, la table de connexions d'un serveur peut être remplie, et les nouvelles requêtes seront refusées. Proposez des solutions pour résoudre ce problème. Analysez les forces et faiblesses de vos solutions.

Bareme : (/40)

exercice	**Note (/40)**
Exercice n°1	8 pts
Exercice n°2	8 pts
Exercice n°3	8 pts
Exercice n°4	8 pts
Exercice n°5	8pts