|  |  |  |
| --- | --- | --- |
| **Niveau :** 03ème Licence ISIL |  | Mardi 29 Mai 2018 |
| **Remarque :** Les réponses doivent être brèves, claires et concises | **Durée**: 1h30’ |

**Université d’Oum El Bouaghi**

**Département des Mathématiques et d’Informatique**

**Module : Sécurité des Systèmes d’Information**

**Examen Final – Corrigé Type**

01 Pt

0.5\*3=1.5

02

0,5\*4=02

1. Définir la sécurité informatique.

La sécurité informatique est **:** l’ensemble de ***moyens*** mis en œuvre pour ***minimiser*** la ***vulnérabilité*** d’un système contre les ***menaces*** ***accidentelles*** ou ***intentionnelles***.

1. Quels sont les niveaux de gestion de la sécurité des systèmes d’information ?

Les niveaux de gestion de la sécurité des systèmes d’information sont : le niveau stratégique, le niveau politique et le niveau procédure.

1. Après la découverte d’une vulnérabilité dans un produit informatique, devons nous publier immédiatement ce point vulnérable ou retarder la publication ? Justifier.

Si on publie la vulnérabilité juste après sa découverte, on risque de divulguer cette information qui est peut être inconnu aux hackers. Cependant, cette publication rend les utilisateurs plus vigilants et peut être considérer une source de pression pour publier le correctif de ce point vulnérable. En conséquence, on doit choisir le bon moment pour la publication de vulnérabilité.

1. Expliquer les étapes d’une méthode d’attaque.

Une méthodologie d’attaque est constitué de :

* 1. Collecte des informations afin de connaître la cible ;
	2. Repérage des failles en consultant les failles recensées, et en éliminant les failles non-fondées.
	3. Intrusion dans le système en prenant des mesures pour ne pas laisser des traces, et en étendant les privilèges.
	4. Assurer l’accès en facilitant l’éventuel retour.
1. Citer et expliquer les types de vulnérabilité.

Les types de vulnérabilité sont :

* 1. Vulnérabilité organisationnelle : les points faibles liés aux procédures de gestion de la sécurité des SI ;

0.25\*04=1

0.5\*4=2

02

01

03

* 1. Vulnérabilité technique : qui est liée à l’utilisation des logiciels et équipements matériels avec les différents problèmes d’interopérabilité et de migration.
	2. Vulnérabilité humaine : l’exploitation des sentiments et comportements humains pour attaquer un SI ;
	3. Vulnérabilité physique : l’ensemble des pannes, des accidents et caractéristiques physiques des salles.
1. Pourquoi la connaissance de l’attaquant et ses motivations est utile dans le cadre de la sécurité des systèmes d’information ?

Connaître l’attaquant peut nous donner des informations sur ses compétences techniques et ses ressources. Connaître les motivations peut nous donner des informations sur les informations et ressources à protéger.

1. Donner un exemple sur l’utilisation des plateformes spontanées.

Utilisation des logiciels libres de VoIP (comme Skype) pour discussion au sein de l’organisation

1. Expliquer en détaille la technique d’attaque pour cartographie un réseau.

Cette technique à pour objectif de déterminer la topologie d’un réseau. Elle est basée sur la commande **tracert** qui permet des déterminer la route entre la source et la cible (c'est-à-dire les adresses des équipements intermédiaires). Cette commande exploite le protocole ICMP et l’information TTL (Time To Life) existante dans un paquet. Donc, en lançant la commande tracert avec l’adresse de diffusion comme paramètre ça nous permet de récupérer tous les équipements intermédiaires dans le réseau.

1. Expliquer les étapes du processus de gestion de risque.



6\*0.5=03

0.5\*3=1.5

1. Quels sont les différentes technologies antivirales ?

Les technologies antivirales sont :

* 1. Analyse de forme,
	2. Contrôle d’intégrité,
	3. Analyse comportementale.

Bon courage !

Dr. Toufik MARIR