|  |  |  |
| --- | --- | --- |
| **Niveau :** 03ème Licence ISIL |  | Mardi 20 Juin 2017 |
| **Remarque :** Les réponses doivent être brèves, claires et concises | **Durée**: 1h30’ |

**Université d’Oum El Bouaghi**

**Département de Mathématiques et d’Informatique**

**Module : Sécurité des SI**

**Examen de Rattrapage – Corrigé Type**

1. Définir la sécurité informatique, la vulnérabilité et la menace.

* ***La sécurité informatique :*** *l’ensemble de* ***moyens*** *mis en œuvre pour* ***minimiser*** *la* ***vulnérabilité*** *d’un système contre les* ***menaces******accidentelles*** *ou* ***intentionnelles****.*
* ***La vulnérabilité*** *est définie comme une* ***faute accidentelle ou intentionnelle*** *introduite dans la spécification, conception ou la configuration d’un système et qui* ***peut être exploité pour créer une intrusion.***
* ***Un attaque*** *est une* ***faute d’interaction malveillante*** *vise à* ***violer une ou plusieurs attributs*** *de la sécurité informatique.*

1. C’est quoi l’ingénierie sociale ?

* L’ingénierie sociale : c’est l’exploitation des failles humaines pour manipuler un utilisateur d’un système informatique afin d’exécuter des tâches utiles pour l’attaquant.

1. Expliquer trois différents types de logiciels malveillants.

* Il suffit d’expliquer trois types parmi les logiciels suivants : Virus, Cheval de Troie, Bombe logique, Portes dérobées, ver.

1. Expliquer les différentes techniques antivirales.

* **L’analyse de forme**: consiste à détecter la présence d’un virus dans un fichier par des caractères statiques qui permettent de le reconnaître. Cette technique utilise, à titre d’exemple, les signatures (qui sont des suites de bits qui caractérisent un virus donné) ou l’analyse spectrale qui consiste à identifier les virus grâce à la présence d’un ensemble d’instructions rarement existent dans des logiciels ordinaires.
* **Le contrôle d’intégrité**: cette méthode consiste à détecter les modifications anormales d’un fichier. Donc, l’anti-virus calcule pour les fichiers sensibles une empreinte infalsifiable. Ainsi, en cas de modification de contenu de fichier, l’anti-virus peut conclure l’existence d’un virus.
* **L’analyse comportementale**: consiste à identifier le virus grâce à un ensemble d’activités suspects comme : l’accès à la table d’interruption, l’accès à des zones spécifiques de système d’exploitation, la tentative d’écriture dans un fichier exécutable, …etc. Donc, un programme qui essaie d’exécuter l’une de ces actions est probablement un virus.

1. Cisco vient de publier un rapport qui mentionne l’existence des failles (zero-day) dans plus de 300 modèles de ses commutateurs (switchs). Ces vulnérabilités ont été découvertes suite à l’étude des documents qui accusent CIA de les tenir secrètes.
   1. Expliquer le concept (zero-day).

* Zero-day : est une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu.
  1. Etes-vous d’accord concernant la démarche de CIA ? justifier.
* Non, Parce qu’il fallait de publier ces vulnérabilités afin de permettre aux développeurs de les corriger.
  1. Quel est le rôle de la « preuve de concept » ?
* Preuve de concept : consiste a démontrer la présence d’une vulnérabilité par l’explication ou la présentation de menaces possibles.

1. Quels sont les critères qu’on peut introduire pour mesurer les risques ?

* Les critères de mesure de risques sont : les menaces, la vulnérabilité et l’impact (Risque = Menace\* vulnérabilité \* Impact).

1. Expliquer, selon les critères de la question précédente, les mesures possibles de traitement des risques.

|  |  |  |
| --- | --- | --- |
| Occurrence de menaces | Impact | Mesures possibles |
| Faible | Faible | Négliger |
| Faible | Elevé | A transférer |
| Elevée | Faible | Accepter |
| Elevée | Elevé | Corriger |

1. Quels sont les motivations possibles d’attaquants ?

* Lupide, Ludique, Terroriste

1. Pourquoi la connaissance de ces motivations est utile dans le domaine de la sécurité des systèmes d’information ?

* La connaissance des motivations de l’attaquant permet de prévoir les objectifs de la sécurité visés et les techniques utilisées

1. Dans quel cas, on supprime l’étape d’exploitation d’une méthodologie d’attaque ?

* Dans le cas d’audit.

 Bon courage !

Dr. Toufik MARIR