Département Informatique Année Universitaire 2015/2016	Université de Tlemcen	3ème Licence (S6) Module Sécurité Informatique

Corrigé Type Contrôle Continu

Note: le corrigé type est donné à titre indicatif. La note attribuée à chaque question/sous question peut varier de 0 à la note complète comme indiqué dans le barème, suivant l'exactitude de la réponse

Exercice 1 (QCM, 13 points, **1,25** par question, sauf **Q1** sur **1,50** et **Q6 1,50**)
Pour chacune des questions suivantes, entourez la bonne réponse ou donner la bonne réponse (case Autre:)

Q1- Un logiciel malveillant
4) Autre: un programme malicieux qui vise à endommager et/ou porter atteinte à un bien ou un système

Q2- Vous avez des données, et vous voulez que personne ne puisse y avoir accès, vous avez donc besoin du service de

4) Autre: Confidentialité

Q3- Vous avez des données stockées sur un support de stockage à lecture seul (ex, CD-ROM). Tant que ces données sont sur ce support, le service suivant est garantit :
2) Intégrité

Q4- Une banque à besoin de s'assurer qui a accès aux comptes de ces clients, depuis quel poste, à quel heure, et quels opérations ont été effectués, elle a donc besoin du service de:

4) Autre: Preuve ou Traçabilité

Q5- un virus infecte

4) Autre: Tout fichier qui peut s'exécuter

Q6- Soit un programme malveillant écrit (code source) en langage Java. Afin que ce dernier puisse endommager une machine infectée il faut que cette dernière dispose de :

4) Autre: Machine Virtuelle Java (JVM)

Q7- Un logiciel malveillant, dont l'apparence est un logiciel saint, mais qui renferme du code malicieux, est :

4) Autre: Cheval de Troie ou Trojan

Q8- Vous recevez un email dans lequel se trouve un lien hypertext, en cliquant sur le lien vous êtes redirigés vers une page Web qui ressemble littéralement au site de messagerie gmail.com, vous êtes probablement en face d'une attaque de type:

4) Autre: Phishing ou hameçonnage

Q9- Un mode de chiffrement par bloc, traite les données à chiffrer

4) Autre: Par bloc de taille fixe

Q10- Soit H une fonction de hachage. Les données en entrée qu'accepte H

3) peuvent être de taille variable

Exercice 2 (3 points, réponse libre)

Sur votre machine, vous arrivez à vous connecter à Internet (Facebook, google, skype, etc.), mais vous constater que votre anti-virus, échoue chaque fois qu'il se connecte à Internet
Q) Selon vous quelle pourrait être la cause? (1,25)
Un logiciel malveillant qui empêche l'antivirus de se connecter à Internet

Pourquoi? (1.75)
Principalement, afin de l'empêcher d'effectuer une mise à jour logiciel, ainsi qu'une mise à jour de la base virale (signature des virus), et ceci pour qu'il ne puisse pas le détecter

Exercice 3 (4 points, réponse libre)
Vous voulez passer une communication vocale numérique (ex, Skype, Viber, etc.) avec une personne distante via le réseau Internet.
Vous avez deux besoins à satisfaire: (1) Vous voulez vous assurer qu'une tierce personne interceptant votre communication ne puisse pas comprendre votre conversation. (2) Vous souhaitez vous assurer que votre conversation est intact (chaque extrémité reçoit réellement ce que l'autre extrémité à dit)
Q1) Citez les services de sécurité dont vous aurez besoin pour satisfaire les deux besoins ci-haut (1) et (2)

(1) service de confidentialité (0,75 pt) (2) service d'intégrité (0,75 pt)

Q2) Quels mécanismes/techniques vont implémenter les services identifiés en Q1 ?
Algorithme de chiffrement pour le service de confidentialité (0,75 pt) , et un algorithme d'intégrité de données pour le service d'intégrité (0,75 pt)

Q3) Pour le service répondant au besoin (1) deux grandes familles existent permettant de l'implémenter, quelle famille est la mieux adapté à notre cas?
Le chiffrement par flot/flux (1 pt)