Faculté des Sciences
Département INFORMATIQUE
Examen du Module : Sécurité Informatique 2019/2020
L3 : SI, ISIL, Par : Dr MA. RIAHLA

Exercice 1 : (Cochez une ou plusieurs bonnes réponses) : (8 points)

1. L'inconvénient de la cryptographie asymétrique est relatif :
   - Au temps de calcul
   - A l'espace de stockage des clés
   - Au partage d'un secret
   - A la vulnérabilité aux attaques classiques
2. Forger un émail consiste à :
   - Envoyer des spams sur le port 25 avec Telnet
   - Ouvrir une connexion avec un serveur SMTP utilisant telnet et soumettre des emails au nom d'un autre utilisateur fictif
   - Se connecter à un serveur SMTP avec Telnet et envoyer un email au nom d'un autre utilisateur existant
   - Voler le compte de messagerie d'un utilisateur
   - Détruire le mail de la victime
3. Une autorité de certification est utilisée pour :
   - Ecarter l'attaque de Man In the Middle
   - Assurer le principe d'authentification
   - S'assurer du propriétaire d'une clé privée
   - S'assurer du propriétaire d'une clé publique
4. La politique de sécurité permet de :
   - Préparer des mécanismes de sécurité
   - Définir le contexte de la politique de sécurité
   - Définir les incidents possibles sur le système à protéger
   - Faire un audit de sécurité
   - Répondre aux incidents de sécurité selon leur fréquence et cout
5. Parmi les étapes d'une porte dérobée on trouve :
   - Installer un keylogger sur la machine de la victime
   - Envoyer un message électronique contenant un ransomware
   - Installer un ver sur la machine de la victime
   - Ouvrir un port sur la machine de la victime et lancer des connexions sur ce port.
6. Je reçois un mail m'annonçant que je peux gagner une caisse de coca. Il suffit d'envoyer un mail à l'adresse qui apparaît dans le message : promo@acces.com. Quelle est la menace possible ?
   - Le pirate tentera de forger mon adresse mail
   - Un spammeur peut me rajouter dans sa liste de victimes
   - Je serai victime d'un cheval de Troie
   - Je suis victime d'un hoax
7. Pour masquer la trace d'un pirate, on utilise
   - Les rootkit
   - La cryptographie
   - L'effacement des fichiers journaux des serveurs
   - Les botnets
8. Le protocole SSH
   - Utilise la cryptographie hybride pour l'administration à distance des serveurs
   - Utilise le HTTPs
   - Remplace le protocole Telnet
   - Est un protocole d'administration à distance

Exercice 2 : (6 points)

1. Pour chaque risque ci-dessous, fournissez les vulnérabilités et montrez s'il s'agit d'un problème de confidentialité (C), d'intégrité (I) ou de disponibilité (D)

Risque	Vulnérabilité	C	I	D
Certains utilisateurs insèrent leurs clés USB non scannées dans les PCs de l'entreprise				
L'entreprise envoie des données sans signatures numériques				
L'entreprise utilise la cryptographie asymétrique sans certificat				

2. Proposez une politique de sécurité (solution) pour chaque ligne

Exercice 2 : (6 points)

1. Chiffrez le message « **Cryptographiemodernes** » avec Vigenère, utilisant la clé « **symetrique** »

2. Donnez 'une clef' de Vigenère qui permet de déchiffrer le message « **BQYPJUVIQZFAGSGWHRGLQ** » pour trouver le mot « **ACLUVWVCMNFINOPDDGCJC**»

3. Soit le texte chiffré : « **cuskqxwmfwituk** », déchiffrez le message par vigenere utilisant les deux clés suivantes :

a. **Bgfbcdfbfdecdg**

b**. quauwtedbdisjg**

c. Quelle est votre conclusion ?

NB : Exercice 1 et Tableau de l'exercice 2 : Réponse sur sujet **……Bon Courage**