Solution td 2

Exercice 1 :

1. *Les techniques d'attaques qui permettent de récolter des informations :*
   Spyware, Keylogger et **Phishing**.
2. *Les techniques d'attaques qui permettent de détourner un système :*
   Backdoors, Rootkit et **ransomware**.
3. *Les techniques d'attaques qui utilisent la messagerie électronique :*
   Canular, Spam et Phishing.
   3.1 *Les caractéristiques communes entre ces attaques :*
   - Message non sollicité.
   - Exploite une vulnérabilité humaine qui est la naïveté des utilisateurs.

   3.2 *Les conséquences nuisibles de chacune de ces attaques :*

• **Canular**	• **Spam**	• **Phishing**
a- Saturation du réseau perte du temps aux utilisateurs. b- Création de la panique chez les utilisateurs (cas de fausse alerte).	Saturation du réseau perte du temps aux utilisateurs	a- Prise en piège des utilisateurs en les incitant à si connecter à des page web trompeuses et saisir de informations sensibles b- Récupération non autorisée des informations sensible (souvent bancaires) c- Prendre l'identité d'une institution financière (banque) ou un site e-commerce.

3.3 l'attaque la plus dangereuse étant le : **Phishing**

Exercice 2 :

1- *Les caractéristiques communes entre un virus, un ver et cheval de Troie sont :*

- Chacun d'eux est un programme malveillant.
- Chacun d'eux compromet l'objectif d'intégrité.

2- *Comparaison entre Virus, ver et cheval de Troie :*

Virus	Ver	Cheval de Troie
Programme **parasite** qui se cache dans le corps d'un autre programme / fichier hôte. ➔ Pas de présence sur le disque dur.	Programme **indépendant** qui n'a pas besoin d'un programme /fichier hôte. ➔ il a une présence dans le disque dur.	Programme **indépendant** qui n'a pas besoin d'un programme / fichier hôte. ➔ il a une présence dans le disque dur.
Un virus se reproduit localement en s'attachants aux fichiers/programmes pour les infecter ➔ il infecte des fichiers /programmes.	Un ver se reproduit de manière **autonome** à travers le réseau en passant d'un ordinateur à un autre ➔ il infecte des ordinateurs/systèmes/réseaux.	Un cheval de Troie ne se reproduit pas ➔ il infecte le système sur lequel est installé.
Il peut dégrader les performances du système dans lequel il est hébergé.	Il peut dégrader les performances d'un réseau entier.	Il peut dégrader les performances du système sur lequel il est installé.

Exercice 3 :

1- Les principes de base de la sécurité informatique compromis par :

- Une attaque passive -> Confidentialité.
- Une attaque Active -> intégrité et disponibilité.

2- <u>Comparaison entre une attaque passive et une attaque active :</u>

	• **Attaque Passive**	• **Attaque Active**
Objectif	Obtenir l'information	1- Modification /fabrication de l'information 2- Perturbation du fonctionnement du système.
Changement	1- Pas de changement de l'état du système. 2- Aucun modification des données	1- Changement de l'état du système. 2- Modification/création illégale de données.
Détection	Souvent difficile à détecter	Facile à détecter grâce aux changements observes

3- Classement des techniques d'attaques employant les programmes malveillants en attaque passive ou attaque active :

Attaque Passive	**Attaque Active**
• Spyware • Keylogger • Phishing	• Virus • Ver • Cheval de Troie • Exploit • Backdoor • Rootkit • Ransomware

<u>Remarque :</u>

Le Phishing peut être facile à détecter. Il faut vérifier l'URL de la page trompeuse écrite dans le navigateur et s'assurer si elle appartient au site prétendu.