TD n° 2 : Menaces et Cybercriminalité

Exercice 1

1. Quelle est la différence entre une vulnérabilité, une menace et une attaque ?
2. Préciser le lien entre ces trois termes.
3. Citer un exemple pour chacun.

Exercice 2 :

Donner le nom de la menace puis préciser si elle est accidentelle ou intentionnelle (passive ou active), informatique ou non informatique :

a) Le serveur de l'entreprise est tombé en panne.
b) Le logiciel de l'entreprise présente une faille de connexion.
c) La salle des serveurs a pris feu.
d) Toufik a oublié de sauvegarder le dernier code qu'il a programmé.
e) Aicha sans faire attention a envoyé un fichier à Amine au lieu de l'envoyer à Amina.
f) Une entreprise cherche à connaître les nouveaux prix fixés pour une autre entreprise concurrente.
g) Amine a supprimé involontairement des informations d'un fichier.
h) Amina a installé sur son ordinateur un logiciel dont elle ne connait pas la provenance.
i) Khaled a introduit de fausses informations dans le système.
j) Ahmed s'est fait passer pour un administrateur pour demander le mot de passe du serveur qu'il a oublié.
k) Sarah a mis volontairement hors service le système d'information.
l) Ali a utilisé un outil pour collecter les informations du réseau.
m) Fatima a copié le flash disque de Yasmina sans son autorisation.
n) L'ordinateur de Khadija a été volé.
o) Omar a dévalisé un compte bancaire.

Exercice 3

Un adolescent de 15 ans « pirate » le système informatique de son collège pour améliorer ses notes. Cet adolescent de quinze ans a été interpellé pour s'être introduit dans le système informatique de son collège dans le but de modifier ses résultats scolaires. Déçu de n'avoir pu atteindre ce but, le collégien a saturé le système informatique en expédiant plus de 40 000 courriels, manœuvre qui a révoqué une indisponibilité du système pendant quatre jours.

1. Citer le type de l'attaquant, sa catégorie ainsi que sa motivation.
2. Discuter les menaces mis en évidence dans cet exemple. Préciser la classe de la menace ainsi que le critère de sécurité correspondant.

Exercice 4 :

Pour chaque cas suivant, donner le nom de l'infection informatique avec justification.

a. CIH, plus connu sous le nom de Tchernobyl a été inventé par un programmeur taïwanais. Le logiciel malveillant remplace le premier Mo de la partition MBR de chaque disque dur appartenant à l'ordinateur par un contenu aléatoire. Le BIOS était également effacé ce qui

rendait la machine inutisable et difficilement réparable. La meilleure solution était de remplacer la carte mère de l'ordinateur et de réinitialiser complètement les disques durs.

b. CryptoLocker est le nom d'un logiciel malveillant s'attaquant aux ordinateurs ayant Windows installé sur leurs machines. Il se propage par email, ensuite il chiffre plusieurs fichiers présents sur la machine. Une fois que tous les fichiers sur l'ordinateur cible sont infectés, il commence à se rependre sur le réseau local pour infecter toutes les machines. Il affiche alors un message disant que pour décrypter les informations, il faudra envoyer un paiement (de 100 à 400 dollars).
c. Morris est l'un des premiers logiciels malveillants distribué via l'Internet. Lancé en 1988 par son créateur, depuis le MIT où il étudié. Il s'appuie sur des vulnérabilités présentes sur les systèmes Unix où les mots de passe sont simples à forcer. Il s'installe alors sur le système et prend des ressources machines à l'utilisateur. Il peut se réinstaller sur un système déjà contaminé et peut causer d'importantes perturbations.
d. Zbot est un programme malicieux qui se présente sous la forme d'un courrier électronique en anglais, prétendument envoyé par le prestataire Internet du destinataire informant ce dernier de la nécessité de mettre à jour ses paramètres de messagerie pour continuer à accéder au service. Si l'utilisateur clique sur le lien hypertexte contenu dans le message, il est redirigé vers une page web qui tente d'exécuter plusieurs scripts malicieux pour infecter l'ordinateur. L'utilisateur est par ailleurs invité à installer un programme nommé settings-file.exe. Si ce fichier est exécuté, le programme s'installe sur le disque dur, modifie la base de registres pour s'exécuter à chaque démarrage de l'ordinateur, puis espionne les frappes entrées au clavier de l'ordinateur contaminé pour tenter de dérober les identifiants d'accès aux sites sécurisés et aux services en ligne tels que les banques.
e. Une personne a reçu un message d'avertissement que les comptes Facebook vont devenir payant ou supprimés si on n'envoie pas le message à 10 personnes ou plus.
f. Une personne a reçu l'email suivant : « Ceci est pour vous informer que vous avez dépassé votre quota de courriel limite de 500MB et vous avez besoin pour augmenter votre limite de quota de courriel parce que dans moins de 48 heures de votre e-mail sera désactiver. Augmenter votre limite de quota de courriel et continuer à utiliser votre compte webmail. Pour augmenter votre limite de quota de courriel à 2 Go, cliquez sur le lien ci-dessous : http://live.outlook.com/login. Nous vous remercions de votre compréhension. »

Exercice 5

1. Décrire les motivations possibles d'une attaque.
2. Quelles classes de menaces (*Interception, Fabrication, Modification, Interruption*) sont impliquées dans les attaques suivantes ?
   a. Attaque de mot de passe par force brute.
   b. Attaque de ping de la mort.
   c. Attaque d'usurpation d'adresse IP.
   d. Attaque de rejeu.
   e. Attaque de Buffer Overflow.
   f. Attaque Bluebug sur un périphérique Bluetooth
   g. Attaque d'usurpation d'identité.
3. Donner pour chaque critère de sécurité les attaques qui lui correspondent :

Disponibilité, authentification, intégrité, confidentialité, non-répudiation.