3ème Année Licence (SI) **2019/2020**

Module : Sécurité Informatique

TD 1 : Introduction à la sécurité informatique

Objectif : enrichir les connaissances de l'étudiant en complétant les informations vues au cours.

Exercice1 : Les programmes malveillants

Un logiciel malveillant (malware en anglais) est un logiciel développé dans le but de nuire à un systèmeinformatique. Nous vous présentons 8 définitions et à vous d'attribuer à chacune le nom du programme malveillant correspondant :

-Def1 : programme se dupliquant automatiquement sur le même ordinateur.Il peut être transmis à un autre ordinateur par l'intermédiaire du courrier électronique ou par l'échangede données ;

-Def2 : exploite les communications réseaux d'un ordinateur afin d'assurer sa reproduction surd'autres ordinateurs ;

-Def3 : programme à apparence légitime qui exécute des routines nuisibles sans l'autorisation de l'utilisateur ;

-Def4 : permet d'ouvrir d'un accès réseau frauduleux sur un systèmeinformatique. Il est ainsi possible d'exploiter à distance la machine ;

-Def5: fait de la collecte d'informations personnelles sur l'ordinateur d'unutilisateur sans son autorisation. Ces informations sont ensuite transmises à un ordinateur tiers ;

-Def6: programme généralement invisible installé sur le poste d'unutilisateur et chargé d'enregistrer à son insu ses frappes clavier pour intercepter des mots de passe par exemple.

-Def7: programme permettant d'exploiter une faille de sécurité d'un logiciel ;

-Def8 : ensemble de logiciels permettant généralement d'obtenir les droits d'administrateur sur une machine, d'installer une porte dérobée, de truquer les informations susceptibles de révéler lacompromission, et d'effacer les traces laissées par l'opération dans les journaux système.

Les noms à attribuer sont : **rootkit, enregistreur de frappe (keylogger), virus, logiciel espion (spyware), ver, l'exploit, cheval de troie (trojan), porte dérobée.**

Exercice2 : Les risques et menaces sur le réseau

Parmi les multiples possibilités de menaces sur le réseau, il y a deux techniques très connues : le « sniffing » et le « spoofing ». Elles ont toutes les deux comme objectif de récupérer des informations sensibles sur le réseau, mais leurs modes de fonctionnement diffèrent. A quoi consiste chaque technique ?

Exercice3 :A savoir « Les risques et menaces du courrier électronique »

S*pam*: un courrier électronique non sollicité, la plupart du temps de la publicité.Ils encombrent le réseau, et font perdre du temps à leurs destinataires ;

Phishing : un courrier électronique dont l'expéditeur se fait généralement passerpour un organisme financier et demandant au destinataire de fournir des informations confidentielles ;

Hoax : un courrier électronique incitant généralement le destinataire àretransmettre le message à ses contacts sous divers prétextes.Ils encombrent le réseau, et font perdre du temps à leurs destinataires.Dans certains cas, ils incitent l'utilisateur à effectuer des manipulations dangereuses sur son poste(suppression d'un fichier prétendument lié à un virus par exemple).

TD 1 : Correction

Exo1 :

1-Virus

2-Ver

3-cheval de troie

4- porte dérobée

5- logiciel espion

6- enregistreur de frappe

7- l'exploit

8- Rootkit

Exo2 :

Les **écoutes** (*sniffing*) : technique permettant de récupérer toutes les informations transitant sur un réseau (on utilise pour cela un logiciel sniffer).
Elle est généralement utilisée pour récupérer les mots de passe des applications et pour identifier les machines qui communiquent sur le réseau.
— **l'usurpation d'identité** (*spoofing*) : technique consistant à prendre l'identité d'une autre personne oud'une autre machine.Elle est généralement utilisée pour récupérer des informations sensibles, que l'on ne pourrait pasavoir autrement.

Exo3 :

Juste à expliquer <u>par les étudiants</u> la différence entre les trois techniques après lecture.