Sécurité des systèmes d'information

TD1

Exercice 1

Question 1
Dans la triade de la CIA, « confidentialité » signifie s'assurer que les données sont :

a. Non accessibles aux parties non désirées.
b. Accessibles de manière anonyme.
c. Correctes et n'ont pas été trafiquées.
d. Disponibles et que les gens puissent y accéder.

Question 2
Dans la triade de la CIA, « intégrité » signifie s'assurer que les données sont :

a. véridiques et honnêtes.
b. non accessibles aux parties non désirées.
c. correctes et n'ont pas été trafiquées.
d. disponibles et que les gens puissent y accéder.

Question 3
Dans la triade de la CIA, la « disponibilité » consiste à garantir que les données sont :

a. non accessibles aux parties non désirées.
b. disponibles pour n'importe qui et n'importe où.
c. correctes et n'ont pas été trafiquées.
d. disponibles et les gens peuvent y accéder.

Question 4
Quelle est la relation entre une vulnérabilité et un exploit ?

a. Un exploit tire parti d'une vulnérabilité pour exécuter un code arbitraire ou obtenir un accès.
b. Ils ne sont pas liés.
c. Une vulnérabilité tire parti d'un exploit pour exécuter un code arbitraire ou obtenir un accès.
d. Un exploit crée une vulnérabilité dans un système.

Question 5
Quelle affirmation est vraie pour un ver et un virus ?

a. Ils s'auto-répliquent et s'auto-propagent.
b. Ils sont indétectables par les logiciels anti-malware.
c. Ils infectent d'autres fichiers avec un code malveillant.
d. Ils ne causent aucun dommage au système cible.

Question 6
Vérifiez tous les exemples de types de logiciels malveillants :

a. Générateurs de clés
b. Vers
c. Virus
d. Adware

Question 7
Quelles sont les caractéristiques d'un rootkit ? Sélectionnez tout ce qui s'applique.

a. Inoffensif
b. Difficile à détecter
c. Fournit des informations d'identification élevées
d. Destructeur

Exercice 2

1. Les attaques nouvelles sur Internet et quand elles n'ont pas encore été classées, sont appelées « attaques de jour zéro, zero-day attacks ». Faire des recherches sur Internet sur les attaques de jour zéro. Qu'as-tu appris ?
2. Quelle est la différence entre un virus et un ver ?
3. Dans quelle mesure les vers sont-ils plus dangereux que les virus ?
4. Certains vers qui se propagent sur Internet ne provoquent aucun dommage sur les machines atteintes. Pourquoi sont-ils cependant nuisibles ?

Exercice 3

Un logiciel malveillant (malware en anglais) est un logiciel développé dans le but de nuire à un système informatique. 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'échange de données ;

-**Def2 :** exploite les communications réseaux d'un ordinateur afin d'assurer sa reproduction sur d'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 système informatique. Il est ainsi possible d'exploiter à distance la machine ;

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

-**Def6:** programme généralement invisible installé sur le poste d'un utilisateur 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 la compromission, 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.**

Exercice 4 :

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 ?

Exercice 5

Dans **les attaques passives** l'attaquant vise à obtenir des informations en transit. Le terme passif indique que l'attaquant ne tente pas de modifier les données. En fait, c'est aussi pourquoi les attaques passives sont plus difficiles à détecter.

Les attaques actives sont basées sur la modification du message d'origine, ou sur la création d'un faux message. Ces attaques ne peuvent pas être prévenues facilement. Cependant, ils peuvent être détectés avec un certain effort.

1. Classer les attaques des scénarios suivant selon la classification précédente
2. Classer les attaques vues en cours selon ces scénarios