Université d'Alger1
Faculté des sciences
Département informatique
Module : Sécurité des systèmes d'information Licence ISIL - 2022/2023

Série 5
Les Attaques informatiques

Exercice 1.

Attribuez à chacun des 8 définitions ci-dessous le nom du malware correspondant parmi les suivants : Rootkit, enregistreur de frappe (keylogger), virus, logiciel espion (spyware), ver, l'exploit, cheval de troie, (trojan), porte dérobée.

-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.

Exercice 2.

Indiquer pour chacun de techniques/moyens d'attaque, décrit dans le tableau ci-dessous, le nom de la technique et l'objectif de sécurité compromis (confidentialité, intégrité, disponibilité et authentification)

- Un attaquant recherche les noms d'employés, des informations sur les produits d'applications logicielles, de marques et de modèles de dispositifs d'infrastructure réseau, etc		
- Un attaquant se place entre deux dispositifs qui		

communiquent pour manipuler les données lorsqu'elles circulent entre eux.		
- Un responsable RH malveillant modifie les informations des feuilles de présence des employés avant de les saisir dans l'application de paie des RH.		
- Des incendies qui ont porté atteinte à l'environnement des serveurs.		
Un attaquant capture les paquets de données en transmission.		
- Un dirigeant malveillant envoie un ordre au nom de son directeur aux autres employeurs.		
- Un attaquant utilise les bots nets pour mener des attaques contre un système cible, en saturant souvent la bande passante.		
- Un attaquant utilise un Keylogger pour enregistre les frappes de l'utilisateur.		
- Un attaquant envoie un message frauduleux (mail de phishing) présenté comme légitime à l'ensemble des		

employés d'une entreprise qui demande de fournir des informations personnelles sensibles		
- Un attaquant envoie de nombreux paquets TCPSYN pour initier une connexion TCP dans le but de saturer le réseau.		
- Un attaquant utilise une fausse adresse IP source pour tromper les systèmes informatiques afin qu'ils acceptent des données de cette source.		
- Un attaquant utilise un script qui teste toutes les combinaisons possibles pour trouver le mot de passe d'un utilisateur victime.		
- Un attaquant tente de voler une petite somme d'argent d'un compte bancaire puis répéter cette action sur un grand nombre de compte.		
- Un attaquant tente de découvrir les services exécutés sur un ordinateur cible en balayant les ports TCP/UDP.		