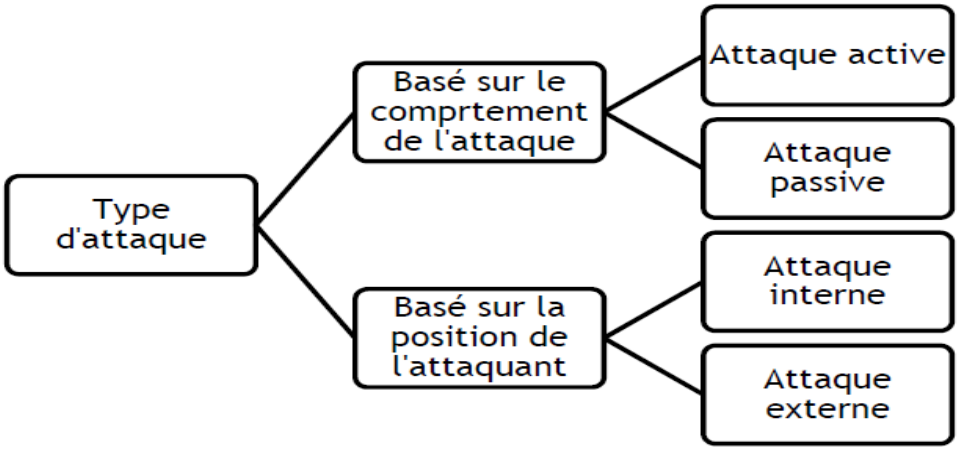
Corrigé TD 2 – Les attaques Informatiques
Exercice 1 :

Compétence	Objectif
• **Script Kiddy** - 90% playstation 9% clickomane 1% intelligence - utilise ce que font les autres • **Amateur** - Failles connues - Failles web • **Professionnel** - En equipe - Avec beaucoup de moyens (financiers, techniques, parfois préparatoires) - 0days possibles	• **L'argent** - piratage volumétrique - cryptolocker "killer application" • **Hacktiviste** - "Terroriste" - Anonymous • **Espions** - Etatique - Industriel • **"Petit con"**



Classification des attaques

3.
• L'attaque browser
• L'attaque brute force
• L'attaque DoS
• L'attaque SSL

4. Kaspersky détecte les attaques en temps réel grâce aux applications suivantes :
• OAS - On-Access Scan (Analyse à l'accès) : OAS affiche un flux de détection de logiciels malveillants lors de l'analyse à l'accès, c'est-à-dire lorsque des objets sont utilisés lors d'opérations d'ouverture, de copie, d'exécution ou de sauvegarde.

• ODS - On-Demand Scan (Analyse à la demande) : ODS affiche le flux de détection de logiciels malveillants lors de l'analyse à la demande, lorsque l'utilisateur sélectionne manuellement l'option 'Rechercher des virus' dans le menu contextuel.
• MAV - Mail Anti Virus : MAV affiche le flux de détection des logiciels malveillants lors de l'analyse de Mail Anti-Virus lorsque de nouveaux objets apparaissent dans une application de messagerie (Outlook, The Bat, Thunderbird). Le MAV analyse les messages entrants et appelle OAS lors de l'enregistrement des pièces jointes sur un disque.
• WAV - Web Anti-Virus : WAVaffiche le flux de détection des logiciels malveillants lors de l'analyse de l'antivirus Web lorsque la page html d'un site Web s'ouvre ou qu'un fichier est téléchargé. Il vérifie les ports spécifiés dans les paramètres Web Anti-Virus.
• IDS - Intrusion Detection System (Scan de détection d'intrusion) : IDS affiche
le flux de détection des attaques réseau.
• VUL - Vulnerability Scan: montre le flux de détection de vulnérabilité.
• KAS - Kaspersky Anti-Spam : KAS affiche le trafic de courrier électronique suspect et indésirable découvert par la technologie de filtrage de réputation de Kaspersky Lab.
• BAD - Botnet Activity Detection (Détection d'activité de botnet): BAD montre des statistiques sur les adresses IP identifiées des victimes d'attaques DDoS et des serveurs C&C de botnet. Ces statistiques ont été acquises à l'aide du système DDoS Intelligence (partie de la Corrigé Kaspersky DDoS Protection).
5. Pour lancer une attaque physique, on peut procéder par :
• Coupure de l'électricité
• Extinction manuelle de l'ordinateur
• Ouverture du boîtier de l'ordinateur et vol de disque dur
• Ecoute du trafic sur le réseau
6. Pour lancer une attaque en réseau, on peut appliquer :
• Des attaques contre le contrôle d’accès, comme War Driving
• Des attaques contre la confidentialité, comme Eavesdropping (Ecoute)
• Des attaques contre l’intégrité, comme 802.11 Data Replay
• Des attaques contre l’authentification, comme VPN Login Cracking
• Des attaques contre la disponibilité, comme AP Theft
7. Pour lancer une attaque DoS en réseau, on peut utiliser :
• l’inondation d’un réseau afin d'empêcher son fonctionnement ;

• la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
• l'obstruction d'accès à un service à une personne en particulier ;
• également le fait d'envoyer des milliards d'octets à une box internet.

Exercice 2 :

a) Les attaques passives ont trait à l'écoute ou à la surveillance des transmissions. Le courrier électronique, les transferts de fichiers et les échanges client / serveur sont des exemples de transmissions qui peuvent être surveillées. Les attaques actives incluent la modification des données transmises et les tentatives d'accès non autorisé aux systèmes informatiques.

b) **Attaques passives** : publication du contenu du message et analyse du trafic.

Attaques actives : masquerade, relecture, modification des messages et déni de service.

c) Les attaques de porte d'entrée exigent les actions d'un utilisateur légitime - par exemple, un logiciel malveillant qui est exécuté lorsqu'un utilisateur légitime ouvre une pièce jointe infectée ou exécute un programme malveillant que l'utilisateur a téléchargé sur Internet.

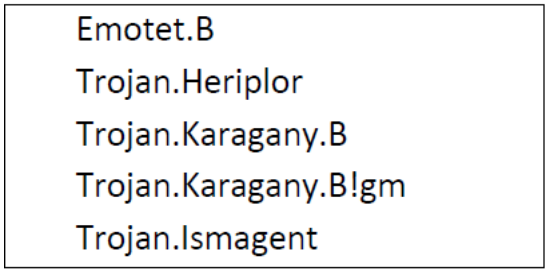
Les attaques de porte arrière ne nécessitent pas les actions d'un utilisateur légitime. Au lieu de cela, ils ciblent les vulnérabilités du logiciel serveur qui exécute un ordinateur. Les défauts dans le logiciel serveur peuvent provoquer un programme serveur pour répondre à une demande inattendue de telle manière qu'il donne accès à l'ordinateur. Une attaque de débordement de tampon (buffer overflow attack) est un exemple d'attaque de porte arrière.

d) Malwares varient considérablement dans les actions qu'ils prennent une fois que cela compromet l'ordinateur d'une victime. Il peut faire n'importe quoi en annonçant sa présence en affichant un message sur l'écran pour que les sons de l'ordinateur jouent.

Il peut également corrompre le système ou tenter d'attaquer d'autres machines en envoyant des courriels infectés, par exemple.

e) Les pirates blancs (white-hat hackers) tentent de rendre les systèmes informatiques plus sécurisés en recherchant et signalant des vulnérabilités afin de pouvoir les réparer. Ils peuvent également aider à caractériser de nouveaux virus et à développer des patchs pour eux.

f) Le 16 mars 2018,



Corrigé TD 3 – Malware
Exercice 1 :
6. Un exploit zero day est une cyberattaque qui survient le jour même où une faiblesse est découverte dans un logiciel. À ce stade, il est exploité avant qu'une solution devienne disponible auprès de son créateur.
Au départ, lorsqu'un utilisateur découvre qu'il y a un risque de sécurité dans un programme, il peut le signaler à la société de logiciels, qui va alors développer un correctif de sécurité pour corriger cette faille. Ce même utilisateur peut également prendre sur Internet et avertir les autres de la faille. Habituellement, les créateurs de programmes créent rapidement un correctif qui améliore la protection du programme, mais parfois, les pirates informatiques entendent d'abord parler de la faille et sont prompts à l'exploiter. Quand cela arrive, il y a peu de protection contre une attaque car la faille du logiciel est si récente.
7. Un virus est un fragment de code qui se propage à l'aide d'autres programmes alors qu'un ver est un programme autonome.
8. L'efficacité des programmes malveillants repose essentiellement à notre époque sur leur capacité à se propager rapidement, en utilisant l'infrastructure des communications.
9. Même s'ils ne provoquent aucun dommage sur les machines, les vers utilisent les ressources du réseau pour se propager, au détriment des communications «utiles».
10. Lors du démarrage d'un ordinateur, c'est généralement le système d'exploitation installé sur le disque dur qui est utilisé par défaut. Il est possible qu'un rootkit ait modifié le secteur d'amorçage ou certaines parties du système d'exploitation pour éviter que le code malveillant puisse être détecté. En conséquence, il est nécessaire d'utiliser un support intègre, par exemple en redémarrant l'ordinateur depuis une clef USB ou un CD-ROM.
Rootkit : un type de malware conçu pour infecter un PC et qui permet au pirate d'installer une série d'outils qui lui permettent d'accéder à distance à un ordinateur.

Exercice 2 :
5. Backdoor : est un cheval de Troie caché dans un logiciel, un service en ligne ou un système informatique entier et dont l'utilisateur n'a pas connaissance. Dans le meilleur des cas, il est créé dès la conception par le développeur du programme, un fournisseur de service ou un constructeur pour réaliser facilement des opérations de maintenance ou pour pouvoir couper l'accès en cas de litige avec un client.
6. L'activation d'une porte dérobée peut se faire au moyen d'un logiciel malveillant de type vers qui va exploiter une faille de sécurité dans le produit et se propager automatiquement à tous les ordinateurs d'un réseau. Plus simplement, le mot de passe par défaut d'un produit peut faire office de backdoor si l'utilisateur ne prend pas la peine de le changer.
7. Le cheval de Troie prend l'apparence d'un logiciel existant, légitime et parfois même réputé, mais qui aura été modifié pour y dissimuler un parasite.
8. - Téléchargement de versions trafiquées sur des sites non officiels ou des plateformes peu sûres (P2P). Télécharger les logiciels sur le site officiel de l'auteur ou du distributeur évite normalement d'avoir affaire à une version infectée par un cheval de trois. Cela n'est évidemment pas possible pour se procurer des versions crackées, mais faisable pour tous les logiciels gratuits.
- Téléchargement de programmes P2P.
- Visite de sites Web contenant un exécutable (par exemple les contrôles ActiveX ou des applications Java).
- Exploitation de failles dans des applications obsolètes (navigateurs, lecteurs multimédias, clients de messagerie instantanée) et notamment les Web Exploit.
- Ingénierie sociale (par exemple, un pirate envoie directement le cheval de Troie à la victime par messagerie instantanée).
- Pièces jointes et fichiers envoyés par messagerie instantanée.
- Connexion d'un ordinateur à un périphérique externe infecté.
- Mise à jour de logiciel.
- Absence de logiciel de protection.

Exercice 3 :

Une première stratégie utilisée par les codes malveillants consiste à empêcher les antivirus de fonctionner correctement. Ceci peut se faire en arrêtant ces programmes ou en bloquant les connexions vers les sites de mise à jour de l’antivirus. Un utilisateur attentif peut remarquer que l’antivirus ne fonctionne plus ou ne se met pas à jour.

Les codes malveillants plus avancés contiennent un rootkit, c'est-à-dire un module qui modifie le comportement du système d'exploitation afin que celui-ci ne divulgue pas la présence du code malveillant. Par exemple, ils vont modifier les appels système utilisés pour lister le contenu d'un répertoire ou les processus actifs afin qu'ils omettent de signaler la présence du code malveillant.

Exercice 4 :

Les antivirus reposent principalement sur deux méthodes fondamentales de recherche de virus : la recherche de signatures et l'analyse comportementale.

-La recherche de signatures consiste à établir la liste de tous les codes malveillants connus et à rechercher leur signature, c'est-à-dire une suite de bits caractéristique, dans des fichiers ou du trafic reçu. Cette méthode ne permet cependant pas de détecter les nouveaux virus encore non répertoriés.

-L'analyse comportementale consiste à étudier le comportement d'un logiciel pour découvrir d'éventuelles actions malveillantes.

L'analyse comportementale nécessite une exécution simulée du code pour pouvoir son fonctionnement. La recherche de signature bénéficie aussi de l'exécution simulée pour détecter une signature qui apparaîtrait seulement après une première étape de décompression ou de déchiffrement de la partie principale du code.

Exercice 5 :

Le code proposé est la version décodée du ver «Anna Kournikova », créé à partir du «VBS Worm Generator» de Kalamar, par un attaquant néerlandais, Jan de Wit. Ce ver ne cause pas de dommage aux données, mais se propage sur Internet via le courrier électronique :

lorsqu'une personne exécute le fichier vbs, celui-ci est envoyé à toutes les personnes figurant dans son carnet d'adresses électroniques.

Accessoirement, si la date courante est le 26 janvier, le programme tente une connexion avec un site Web des Pays-Bas : www.dynabyte.nl

-Plus précisément, le programme effectue des changements dans la base de registre, créant une entrée nommée HKCU\software\OnTheFly. Cette entrée, initialisée à made with Vbswg 1.50b, prendra la valeur 1 lorsque le programme sera exécuté.

-Le programme se copie dans le répertoire Windows.

-Si le programme est exécuté pour la première fois (HKCU\software\OnTheFly ne vaut pas 1), alors on applique la procédure Infect().

-Si la date courante est le 26 janvier, alors le ver essaie de se connecter au site www.dynabyte.nl
-Enfin, le programme teste dans une boucle infinie si le fichier est effacé : s'il est effacé, alors il est créé de nouveau.
-La fonction Infect() propage le courrier électronique en l'envoyant à l'ensemble des adresses électroniques contenues dans le carnet d'adresses.

Exercice 6 :

1. L'installation d'un antivirus permet de protéger le système informatique des virus actuellement connus. Il est donc primordial de mettre à jour son antivirus dès que l'éditeur en offre la possibilité. Cependant, même en effectuant ces mises à jour, le système n'est pas à l'abri des nouveaux virus, qui ne sont pas encore reconnus par les antivirus.
2. Si les produits antivirus des grandes marques sont tous capables de reconnaître l'ensemble des virus connus, ils ne sont pas tous aussi réactifs lors de la découverte d'un nouveau virus. Certains produits proposeront des mises à jour plus rapidement que d'autres.