### Exercice 1 :

|  |  |
| --- | --- |
| **Termes** | **Définitions** |
| Antivirus | (d) |
| Pare-feu | (e) |
| IDS | (a) |
| DMZ | (c) |
| Proxy | (b) |

### Exercice 2 :

* L’anti-virus fait un analyse/scan de l’ordinateur (fichiers, exécutables), l’opération d’analyse est fait par un moteur de scan « *Scan Engine* », Il scanne les informations et si les virus sont détectés, il les désinfecte. Les informations peuvent être numérisées de différentes manières[[1]](#footnote-1) :
  + Il compare la taille de fichier avant et après l’infection
  + « *Pattern Matching* », Il cherche si la signature d’un virus est existante dans la base de données des signatures des virus connu.
* Le fonctionnement de pare-feu est basé sur le principe du filtrage simple des paquetés « *Stateless Packet Filtring* » entante / sortant de réseau, il analyse les en-têtes de chaque paquets contre un ensemble des règles qui les autorise ou les refuse d’entre dans le système.
* IDS écoute le réseau (*N-IDS*) d’une manière furtif afin de repérer des activités anormales ou suspectes, il capture une copie des paquets et vérifie les points suivants[[2]](#footnote-2) :
  + « *Anomaly Detection* », par exemple, la vérification de la pile protocolaire, il vérifier les paquets non respectons (violation) de les normes / protocoles (IP, TCP, UDP, ICMP)
  + « *Signature Match* », il compare le paquet avec une base de données des signature, alors, l’IDS lance une alerte l’ors un comparaissant positive.

### Exercice 3 :

1. **Exemples de méthodes d’infection par un Cheval de Troie :**

* Téléchargement dès l’logicielle ou jeux vidéo cracker (utilisation des sites torrent) qui peuvent contenir des Trajan.
* Lecture des clés USB d’origine inconnue.
* Fichiers jointes envoyée par les systèmes de chat ou e-mail



* Ne télécharge / installe jamais des logiciels cracker ou sans avoir une vraie licence (case des logicielles payantes).
* Utilisations des antivirus à jour.

1. **Déférence entre un cheval de Troie et un virus :**

|  |  |
| --- | --- |
| **Virus** | **Cheval de Troie** |
| * Malware capable de se reproduire en s’insérant dans un host. | * Malware non reproductible a pour objectif d’accès non autorisé (exemple : backdoor) |

1. **Type des Trajan[[3]](#footnote-3) :**

* Remote Access Trojans – RAT (Backdoor Trojan)
* FTP Trojans
* Data Sending Trojans
* Proxy Trojans
* DDOS Trojans

### Exercice 4 :

|  |  |  |
| --- | --- | --- |
| **N° Texte** | **Solutions** | |
| **1** | **Q1** | * Social Engineering Attack, |
| **Q2** | * Utilisation d’un fournisseur reputable de nom de Domain (Google Domains, bluehost) qui garantit la service de protection des informations privées «WHOIS Privacy Protection Service » |
| **2** | **Q1** | * Social Engineering Attack |
| **Q2** | * Backup * Activation de « Two Factor Authentication » dans tous les comptes s’il est possible. |

1. https://www.researchgate.net/profile/Sarika\_Choudhary/publication/308800880\_How\_Anti-virus\_Software\_Works/links/57f333f508ae91deaa590343/How-Anti-virus-Software-Works.pdf [↑](#footnote-ref-1)
2. IDS vs. IPS : https://www.youtube.com/watch?v=rvKQtRklwQ4 [↑](#footnote-ref-2)
3. [*https://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/what-is-a-trojan-horsee*](https://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/what-is-a-trojan-horsee) [↑](#footnote-ref-3)