TD 1 – Initiation à la Sécurité Informatique

Exercice 1 :

1. Quels sont les différents types de sécurité étudiés au cours ?
2. Identifiez les exigences fondamentales en sécurité informatique. Puis, expliquez la différence entre eux.
3. Présentez les mécanismes de sécurité définis dans X.800.
4. Aujourd'hui, les chercheurs en sécurité informatique s'intéressent davantage au "Privacy" ? Est-ce que peut-on la classifier comme une exigence de sécurité ?
5. Quels sont les services offerts par le contrôle d'accès ?

Exercice 2 :

1. On a vu au cours que l'authentification est un moyen pour vérifier ou pour prouver l'identité d'un utilisateur. Cependant, l'utilisateur doit il présenter quelles informations pour prouver son identité ?
2. Quel est la différence entre authentification, authentification à deux facteurs, et authentification à trois facteurs ? Donnez des exemples.
3. Présentez le schéma "*Authentification vs. Autorisation*" vu au cours.
4. Quels sont les différents types d'intégrité.
5. Dessinez une matrice semblable au tableau 1.3 (vu au chapitre 1) qui montre la relation entre les services de sécurité et les attaques.
6. Dessinez une matrice semblable au tableau 1.3 (vu au chapitre 1) qui montre la relation entre les mécanismes de sécurité et les attaques.

TD 2 – Les attaques Informatique

Exercice 1 :

1. Classifiez les attaquants par compétence, puis par objectif.
2. Donnez deux classifications standard (vu au cours) pour les attaques. Cependant, vous pouvez proposer une nouvelle classification et cela n'est possible qu'à après l'étude de tous les attaques.
3. Nous avons vu au cours les attaques réseaux (les plus fréquentes) publié par McAfee Labs en 2016. Donnez quatre attaques les plus fréquentes.
4. Basé sur l'application du map développée par kaspersky (https://cybermap.kaspersky.com/), on a pu voir au cours les attaques en temps réel. Comment sont-elles détectées en temps réel ?
5. Donnez quatre scénarios pour lancer une attaque physique.
6. Donnez trois scénarios pour lancer une attaque en réseau.
7. Donnez un scénario pour lancer une attaque DoS en réseau.

Exercice 2 :

1. Quelle est la différence entre les menaces de sécurité passives et actives?
2. Listez et définissez brièvement les catégories d'attaques de sécurité passives et actives.
3. En classe, nous avons fait la distinction entre une attaque de porte d'entrée et une attaque de porte arrière (front-door attack and a back-door attack). Expliquez comment ils sont différents et donnent un exemple de chacun.
4. Donnez des exemples de ce que le malware tente d'accomplir.
5. Décrivez les façons dont les pirates blancs (white-hat hackers) tentent de rendre les systèmes informatiques plus sûrs.
6. Accédez au site Symmantec Security Response à l'adresse suivante:

   Http://securityresponse.symantec.com/

   Voir la liste des dernières menaces de virus. Quels sont les noms des cinq premiers?