TD1 : Sécurité des réseaux

1. **Donnez les cinq principaux services de sécurité avec une définition de chaque service ?**

- **Contrôle d'accès** : limiter l'accès au système. Seules les personnes autorisées aient accès aux ressources
- **L'authentification** : S'assurer (vérifier) de l'identité de l'utilisateur
- **L'intégrité** : Détecter toute modification des données.
- **La confidentialité** : assurer que l'information n'est divulguée (dévoilée ou révélée) qu'aux personnes autorisées.
- **La disponibilité** : permettant de maintenir le bon fonctionnement du système d'information.
- **La non répudiation** : permettant de garantir qu'une transaction ne peut être niée ;
- **Fraîcheur** :

2. **Donnez pour chaque service (citez dans Q1) de sécurité l'attaque (les attaques) qui lui correspond ?**

Les services	Les attaques
Contrôle d'accès	
L'authentification	Usurpation d'identité
L'intégrité	Modification de l'information
La confidentialité	Écoute et Interception des messages sur le réseau
La disponibilité	Déni de service (DoS) Bombardement
La non-répudiation	Répudiation
Fraîcheur	Rejoue de message

3. **Donnez pour chaque service un moyen permettant de lui réaliser ?**

Les services	Moyens
Contrôle d'accès	• Filtrage réseau (par adresse MAC ou adresse IP, par nom de domaine) • Donner un mot de passer pour un réseau wi-fi

L'**authentification**	• Login/mot de passe • Certificat
La **confidentialité**	Chiffrement des données
L'**intégrité**	Ajout de champ MAC ou MIC
La **disponibilité**	
La **non répudiation**	Signature numérique
Fraîcheur	• time-stamp (date) • nonce

4. **Quelle est la différence entre une attaque active et une attaque passive ? donnez un exemple pour chaque type d'attaque ?**

- Les attaques passives : consistent à écouter sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais une prévention est possible.
- Les attaques actives : consistent à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau. Noter qu'une attaque active peut être exécutée sans la capacité d'écoute.

5. **Citez Trois principaux domaines où la sécurité est une chose primordiale (indispensable) ?**

- Domaine commerciale (site de ventes et achat, réseau d'une banque, etc…)
- Domaine militaire
- Domaine médicale

6. **Quelle est la différence entre un virus, un ver, et un espion ?**

Un virus est un logiciel malveillant conçu pour se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme les réseaux informatiques et les cédéroms, les clefs USB.

Un ver, contrairement à un virus informatique, n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.

Un espion est un logiciel malveillant qui infecte un ordinateur dans le but de collecter et de

transmettre à des tiers des informations de l'environnement sur lequel il est installé sans que l'utilisateur n'en ait conscience.

Exercice N°1

Définir les mots suivants :

- Authentification : a pour but de vérifier l'identité dont une entité (personne ou machine) se réclame. Généralement, l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté.
- Confidentialité : a été définie par l'Organisation internationale de normalisation (ISO) comme « le fait de s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé », et est une des pierres angulaires de la sécurité de l'information.
- Intégrité : désigne l'état de données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation.

1. **Décrire l'attaque de web spoofing**

Web Spoofing est une attaque de sécurité qui permet à un adversaire d'observer et de modifier toutes les pages Web envoyés à la machine de la victime, et d'observer toutes les informations entrées dans les formulaires par la victime. Web Spoofing travaux sur les deux principaux navigateurs et n'est pas empêché par "sécuriser" les connexions. L'attaquant peut observer et modifier toutes les pages Web et la soumission de formulaire, même lorsque le navigateur "connexion sécurisée" est allumé. L'utilisateur ne voit aucune indication que quelque chose ne va pas.

4. Décrire deux variantes de l'attaque de déni de service.

* l'inondation d'un réseau afin d'empêcher son fonctionnement

* la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier

*brouillage de signal radio pour mettre réseau wi-fi hors service.