TD1 : Sécurité des réseaux

Ch1 : Principes de sécurité

1. **Donnez les cinq principaux de sécurité avec une définition succincte de chaque service ? (0,5 pour le nom de service, 1 point pour la définition). (7,5 points)**

- **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 ? (répondre sous forme de tableau) (1 points par attaque) (5 points)**

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 ? (5 points)**

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 ? (4 points)**

- 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) ? (3 points)**

- 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.

7. **Comment peut-on réaliser l'attaque de déni de service (DoS : Denial of Service) dans :**
   a. **un réseau local Ethernet :** Sniffer
   b. **un réseau sans fil :** jamming
   c. **un serveur web :** Spoofing

8. **Citez les différentes attaques informatiques que vous connaissez ?**

- Accès physique
- Interception de communications
- Dénis de service
- Intrusions
- Ingénierie sociale
- Trappes

Exercice N°1

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.

2. 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.

Some english definition:
Web spoofing allows an attacker to create a "shadow copy" of the entire World Wide Web. Accesses to the shadow Web are funneled through the attacker's machine, allowing the attacker to monitor the all of the victim's activities including any passwords or account numbers the victim enters. The attacker can also cause false or misleading data to be sent to Web servers in the victim's name, or to the victim in the name of any Web server. In short, the attacker observes and controls everything the victim does on the Web.

More about web spoofing:
http://www.cs.princeton.edu/sip/WebSpoofing/
http://en.wikipedia.org/wiki/Spoofing_attack

3. Comment peut-on réaliser l'attaque de smurf

Une attaque smurf n'est pas très sophistiquée. Il suffit d'un routage pirate, et le protocole IP fait ensuite tout le travail. L'attaque se déroule généralement en cinq étapes:

1. Le hacker identifie l'adresse IP de la victime (votre serveur web constitue généralement une cible parfaite).
2. Il repère un site intermédiaire qui va amplifier l'attaque (en général il en choisit plusieurs pour mieux masquer son attaque).
3. Il envoie un fort trafic ICMP (ping, couche 3) à l'adresse de transmission des sites intermédiaires. Ces paquets présentent une adresse IP source falsifiée désignant la victime.
4. Les intermédiaires envoient la transmission de la couche 2 vers tous les systèmes hôtes de leurs sous réseaux.
5. Les systèmes hôtes répondent au réseau victime.

Autre définition :

Technique courante d'attaque par déni de service, mais utilisant une approche différente de l'attaque par déni de service classique. L'attaque par déni de service utilise normalement des pings par défaut pour « submerger »un hôte donné. Mais pour vraiment submerger les ressources d'une cible donnée, l'attaquant doit corrompre de nombreux ordinateurs, et leur faire envoyer des requêtes ping simultanément.

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.

Exercice N°2

Choisissez les réponses justes aux questions posées.

1. Un virus :
   a- Est un logiciel malveillant qui est doté de l'autonomie et se duplique à travers un réseau
   b- Est un programme qui s'installe dans un autre programme et qui se duplique grâce à celui-ci
   c- Est un logiciel dont l'objectif premier est d'espionner

2. Le spamming :
   a- Est une variante du ping flooding
   b- Permet de saturer la boite à lettre d'une victime par un nombre important de courrier électronique
   c- Est une variante du mail-bombing

3. Le déni de service est une attaque contre :
   a- la confidentialité
   b- l'intégrité
   c- la disponibilité

4. Une fonction de hachage :
   a- Produit une empreinte de longueur fixe
   b- Produit une empreinte de longueur quelconque
   c- Est irréversible

5. Le chiffrement asymétrique assure :
   a- La non-répudiation.
   b- L'intégrité
   c- La confidentialité, l'authentification et l'intégrité
   d- La confidentialité

6. Le phishing est :
   a- Un programme installé sur le poste d'un utilisateur pour enregistrer à son insu ses frappes clavier
   b- Une technique essayant d'extraire des informations confidentielles sur un client
   c- Une technique qui tente d'entraîner un client d'une banque vers un site web qui ressemble très fort à celui de sa banque

---

- Le **mail-bombing** est une technique d'attaque visant à saturer une boîte aux lettres électronique par l'envoi en masse de messages quelconques par un programme automatisé. On utilise les termes de *mail-bomber* pour caractériser l'action de faire du *mail-bombing* (de saturer de messages/courriels) et de *mail-bomb* pour le courrier reçu sous cette forme et dans ce but.
-