Chapitre 1:
Introduction à la sécurité info

Types de sécurité

- Sécurité des données
- Sécurité des réseaux
- Sécurité d'internet
- Sécurité informatique

Objectifs de la sécurité:

- disponibilité: l'information sur le système soit disponible aux personnes autorisées.
- confidentialité: l'information sur le système ne puisse être lue que par les personnes autorisées.
- intégrité: l'information ne puisse être modifier que par les personnes autorisées.
- non répudiation: permettant de garantir qu'une transaction ne peut être niée.
- authentification: consiste à assurer que seules les personnes autorisées aient accès aux ressources.

SI

Le contrôle d'accès:

- authentification
- autorisation
- responsabilisation

Types de contrôle d'accès:

- centralisé
- décentralisé

- pour prouver l'identité l'utilisateur doit présenter l'une des informations suivantes:
  - ce que vous savez (mdp, PIN)
  - ce que vous avez (Jeton, cartes à puce, RFID).
  - qui vous-êtes (empreintes digitales, signature ...).

* Authentification basée sur la biométrie

physiologique humain (exp: empreintes digitales)

comportement (exp: signature)

Authentification → à deux facteurs.
" → 3 "
" → multi "

Intégrité

des données
La propriété que les données n'ont pas été modifiée d'une manière non autorisée.

du système.
La qualité du système lorsqu'il exécute sa fonction prévue de manière intacte, sans manipulation non autorisée.

* L'attaque: est l'exploitation d'une faille d'un système informatique à des fins non connues par l'exploitant du système et généralement préjudiciables.

Types des attaquants :

par compétence :
- script kiddy
- Amateur (failles web)
- professionnel (en equipe)

par objectif :
- d'argent
- Hacktiviste
- espions
- "Petit con"

- définition d'attaque : c'est une tentative d'exposer, de modifier, de désactiver, de détruire, de voler ou d'obtenir un accès non autorisé.

Type d'attaque :

Basé sur le comportement de l'attaque
- active
- passive

Basé sur la position de l'attaque
- interne
- externe

chapitre 2:

Les protocoles de sécurité.

- Le protocole de sécurité: c'est un ensemble de règles régissant le comportement d'individus pour répondre aux besoins d'une application.
- pour sécuriser les msg ⟹ utiliser la cryptographie.
- La cryptographie: un ensemble de méthodes permettant de chiffrer un msg numérique, grâce à une clé.

chiffrement

Symétrique: une seule clé pour chiffrer / déchiffrer.

Asymétrique: une clé pour le chiffrement, et une autre pour le déchiff.

- Les fonctions de hachage sont généralement utilisées pour garantir l'intégrité.

cryptographie

Sans clé

- Les fonctions de hachages.
- séquences aléatoires.

Avec clé.

- chiff symétrique
- chiff Asymétrique.

- protocole AAA:

- AAA correspond à un protocole qui réalise 3 fonctions: l'authentification, l'autorisation, la traçabilité.

- AAA est un modèle de sécurité implémenté dans certains routeurs cisco ou certains switches Alcatel.
- AAA est la base des protocoles de télécommunication Radius et Diameter.
- Radius et diameter sont utilisés dans les réseaux mobiles UMTS et LTE pour authentifier et autoriser l'accès des terminaux mobiles au réseau.

RADIUS:

- protocole standard d'authentification, défini au sein des RFC 2865 et 2866.
- Le fonctionnement basé sur un système client / serveur chargé de définir les accès d'utilisateurs distants à un réseau.
- ce protocole permet de faire la liaison entre des besoins d'identification et une base d'utilisateurs en assurant le transport des données d'authentification de façon normalisée.
- RADIUS connaît 2 protocoles de mots de passe :
  - PAP : échange en clair du nom et du mot de passe).
  - chap : échange basé sur un hachage de part et d'autre part avec échange seulement du "challenge".
- Le protocole prévoit 2 attributs séparés : user password et chap_password
- chap est un protocole d'authentification pour PPP (point_to_point protocol) à base de challenge.

Diameter :

- est un protocole d'authentification, successeur du protocole RADIUS.
- il est défini par RFC 3588, et définit les pré-requis minimums nécessaire pour un protocole AAA.
- il est utilisé dans les réseaux de téléphonie mobile pour accéder aux bases de données HLR et HSS permettant d'identifier, d'authentifier et de localiser les abonnés mobiles 3G et LTE/4G.
- Le protocole Diameter est basé sur les messages (paquets).
- Il existe 2 types de messages : → Le message request.
  → Le message answer.
- Les AVP de Diameter sont l'unité de base dans le msg Diameter qui contient les données (d'authentification, de sécurité, ... etc).
- Il doit y avoir au moins un AVP à l'intérieur du msg Diameter.
- La structure de l'AVP Diameter contient :
  1. code AVP (4 octets)
  2. drapeaux
  3. AVP longueur : indique le nombre d'octet dans l'AVP.
  4. fournisseur ID.

Le protocole EAP :

- est un protocole de communication réseau embraquant de multiples méthodes d'authentification, pouvant être utilisé sur les liaisons point à point (RFC 2284), les réseaux filiaires et les réseaux sans fil (RFC 3748,

RFC (2473) tq les réseaux wifi.

- L'infrastructure EAP est constituée de :
  1. homologue EAP.
  2. Authentificateur EAP.
  3. Serveur d'authentification.