Chapitre 1: Notions de base

1) Introduction

* Se connecter à internet : Les ressources informatiques sont exposées à divers "dangers".

* Sécurité : L'étude de 3 principaux axes :

  - Attaques
  - Services ou objectifs
  - Mécanisme de sécurité (la solution)

2) Attaques et Logiciel

a) Les programmes malveillants (Déjà developpés)

Un logiciel malveillant (malware) est un logiciel developpé dans le but de nuire à un système informatique

- Le virus : Programme (un bout de code) intégré dans un autre programme afin de perturber le fonctionnement d'un système il propage lors de l'échange des données (support de stockage).

- Le ver (Worm) : Contrairement aux virus c'est un programme qui est développé pour se propager automatiquement d'un système à un autre dans différents équipements réseau afin de saturer les ressources (les mémoires, les débits, les bandes passantes...). Il se propage automatiquement dès qu'il se connecte sur un réseau.

- Le cheval de troie (trojan) : a pour but de pénétrer dans un système afin d'ouvrir des failles = des sessions, des ports ...
  * programme à apparence légitime (permis) qui exécute des routines nuisibles sans l'autorisation de l'utilisateur

- La porte dérobée (backdoor) : même objectif (3) que trojan.
  * Exploiter la machine à distance.
- Le logiciel espion (spyware) :
  * Son objectif est de collecter des informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation.
  * Collecter le trafic échangé entre les équipements deux
- L'enregisteur de frappe (Keylogger).
  * Collecter des informations personnelles
  * Collecter les frappes clavier, pour intercepter des mots de passe par exemple.
- L'exploit : Son objectif est de chercher/exploiter une faille de sécurité d'un logiciel
- Le root kit : Son objectifs c'est d'avoir les privilèges de l'administrateur pour installer, télécharger, truquer des informations ...

b) Les risques et menaces : (des scénarios)

Les attaques réseaux

Une attaque passive

* ne modifie pas l'état de communication ou du réseau
- Observation par sonde et l'analyse de trafic
- Collecte d'informations.

Une attaque Active

* dangereuse, car elle modifie l'état d'un serveur ou l'état d'une communication

* Une attaque peut être interne / externe

3) Services et Objectifs

a) => Qu'est ce que je dois assurer ?

C I A = protection

1) Confidentialité : cacher les données circulées entre source et destinataire
2) Integrité : Assurer que les données sont bien envoyées correctement (= chiffrer)
3) Disponibilité : Assurer que les services sont toujours disponible

* Pour chaque attaque on a des objectifs

Objectifs :

* L'Authentification : Consiste à assurer l'identité d'un utilisateur (Signature), garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.
* La non répudiation du message : l'émetteur ne pourra pas nier avoir envoyer le message.
* Contrôle d'accès : Consiste à vérifier si une entité (une personne, un ordinateur, ...) demandent d'accéder à une ressource à les droits nécessaires pour le faire.
* Identification :

permet de connaître l'identité d'une entité, souvent à l'aide d'un identifiant.

b) Terminologie :

1) • Vulnérabilité := Les faiblesses / failles
   • Les points faibles d'un système.
   Exemple : faiblesse de performance.
   * Elle existe principalement
   • défaut de configuration
   Exp : comptes par défaut ; ORACLE

- Exp2 : CISCO : un serveur Web active par défaut
- Une configuration typique (checklist)

- Protocoles de communications :

Exp1 : ARPSpoof exploite une faille au niveau du protocole ARP

Exp2 : SYNflood exploite une faille au niveau du protocole TCP.

- Erreur de programmation :

Exp1 : Buffer overflow

Exp2 : SQL ~~(ject)~~ injection

2) • Risque : L'exploitations de vulnérabilité sur un système.

Exp : J'ai une vulnérabilité ⇒ Quel est le risque ? Sur le système

Afin de réduire le danger à des niveaux acceptables, c'est à dire pour assurer la protection, il faut :

* Résoudre les menaces
* Réduire les facteurs de vulnérabilité
* Augmenter les capacités de protection

Vital :
La nature du risque peut mettre en cause la survie de l'entreprise

Critique
La nature du risque peut affecter durablement les performances économiques de l'entreprise

Sensible
La nature du risque peut affecter l'entreprise de manière non négligeable même si limitée dans le temps

non critique
Coût lié au risque existant mais limité.

3) • Contre-mesures

* Les solutions pour les risques
* pour chaque risque on identifie les contre-mesures
* Les solutions peuvent être des matériels, et logiciels de sécurité. / La compétence des administrateurs sécurité. / La formation des utilisateurs / Les Lois en vigueur.

• Les contre-mesures peuvent être

Administratives

* prévenir
* detecter
*. Corriger
* récuperer

} Les rôles des contre-mesures

Techniques
- Antivirus

physiques

4) Menace

* Source de risque interne/externe
* Concerne aussi bien le hardware/software
* Visant les données / les utilisateurs / la documentation
* d'origine : naturel / humaine (hacker)

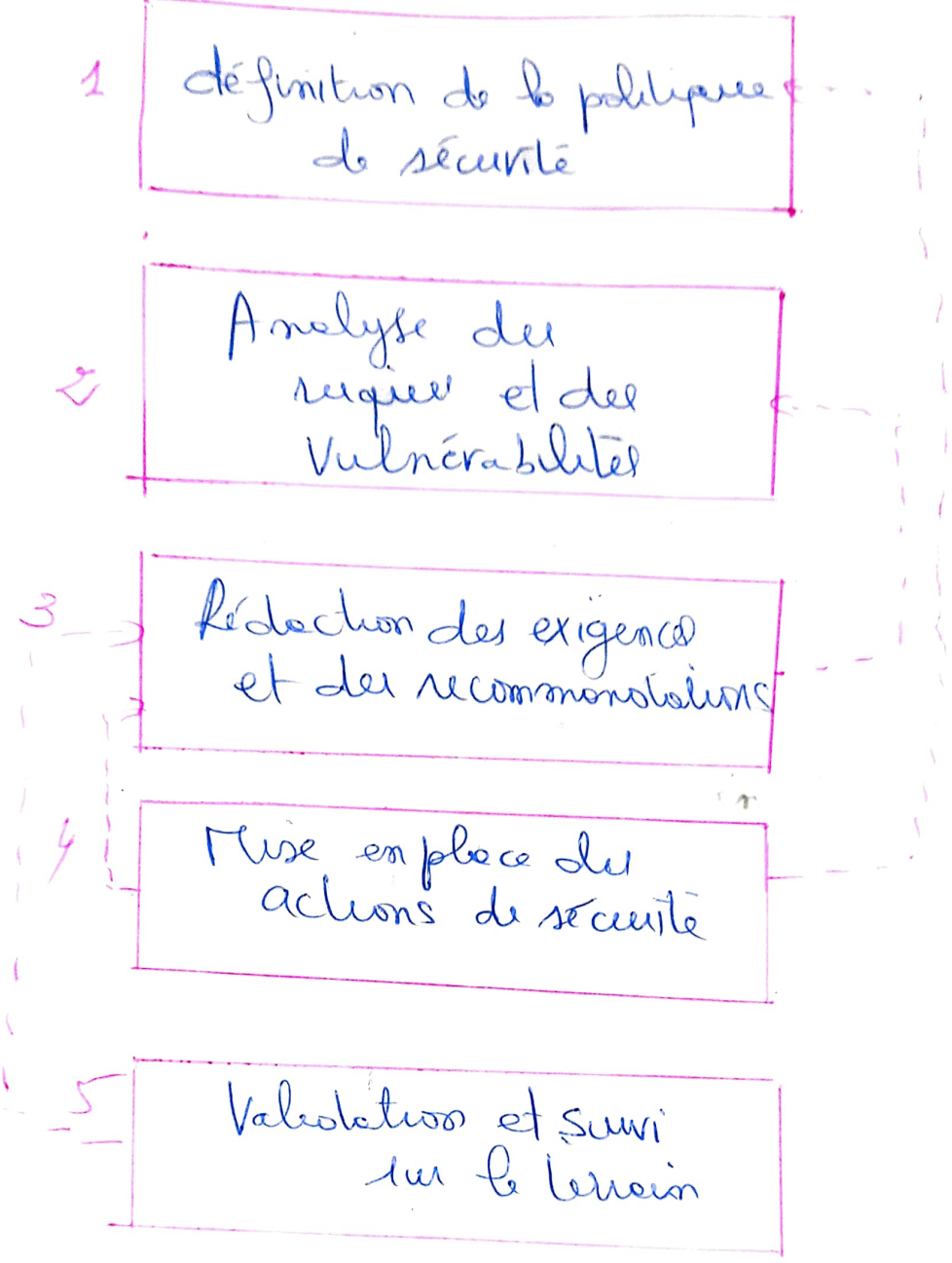
5) Impact :

* Les conséquences d'une menace sur l'organisme
* il peut être fort ou bien faible

= outil

4) Mécanisme de sécurité :

1) Identification des menaces
   * Qui ou Quoi ?
   * Comment (Vulnérabilités) ?
2) Evaluer les risques :
   * Probabilité
   * Impact
3) Considérer les mesures de protection par rapport au risque :
   * Efficacité
   * coût
   * difficulté d'utilisation
4) Mettre en place et opérer les mesures protection



1 - Répond.

- Qui ? Peut ? Connaître ? Quoi ?
  Doit modifier
  Ne Doit pas communiquer
- Quelle sécurité appliée à l'information ?
- Comment le faire ?
- Quels moyens pour atteindre cet objectif ?

2. Analyser les risques

- prendre en compte les menaces
- Les points sensibles
- Les actifs de l'entreprise

Les règles de base :

* Interdiction par défaut :
  - tout ce qui n'est pas autorisé explicitement est interdit
* Moindre privilège :
  - N'autorise que le strict nécessaire
* Défense en profondeur :
  - Protéger au plus tôt et à tous les niveaux.
* Goulet d'étranglement :
  - Centralisation de la sécurité
  - Acceptation des contraintes par les utilisateurs