Sécurité des Systèmes d'Information

(Vulnérabilité, menace et attaque informatique)
Partie 1: Initiation aux attaques informatiques

université d'Alger 1 -
Benyoucef Benkhedda

Objectifs du chapitre:

- Apprendre la méthodologie d'une attaque
- Apprendre les différentes attaques informatiques

Intrusion (attaque)

Une intrusion peut être définie comme tout ensemble d'**actions** qui essayent d'exploiter une ou plusieurs **failles** du système à travers une ou plusieurs **menaces** détectée afin de compromettre :

- **Confidentialité:** exemple vol de données furetage, fuite d'informations par canal caché
- **Intégrité:** exemple modification illégitime de fichiers
- **Disponibilité:** exemple occupation illégitime ou abusive de ressources, destruction illégitime ou abusive de fichiers)
- **Authenticité:** exemple vol de brevets scientifiques des inventions

Menace:

- ✓Est un **danger** qui existe dans l'environnement du système **indépendamment** de ce dernier.
- ✓Peut être une **intention** exprimée ou démontrée de nuire ou de rendre indisponible un actif.
- ✓Les circonstances extérieures, l'erreur humaine ou la négligence sont également considérés comme des menaces.
- ✓Elle peut présenter: accident, erreur, malveillance (passive ou active)

Vulnérabilité (faille):

✓Présente un **défaut** dans le système (dans sa construction, configuration ou conception) qui expose le système à des menaces possibles.

✓Elle peut être:

- Bugs dans les logiciels
- Mauvaises configurations
- Services permis et non utilisés
- Virus et chevaux de Troie
- Saturation de la liaison d'accès à l'Internet
- Logiciels en mode debug

✓ Voir https://www.cvedetails.com/

Intrusion (attaque)

Pourquoi attaquer?

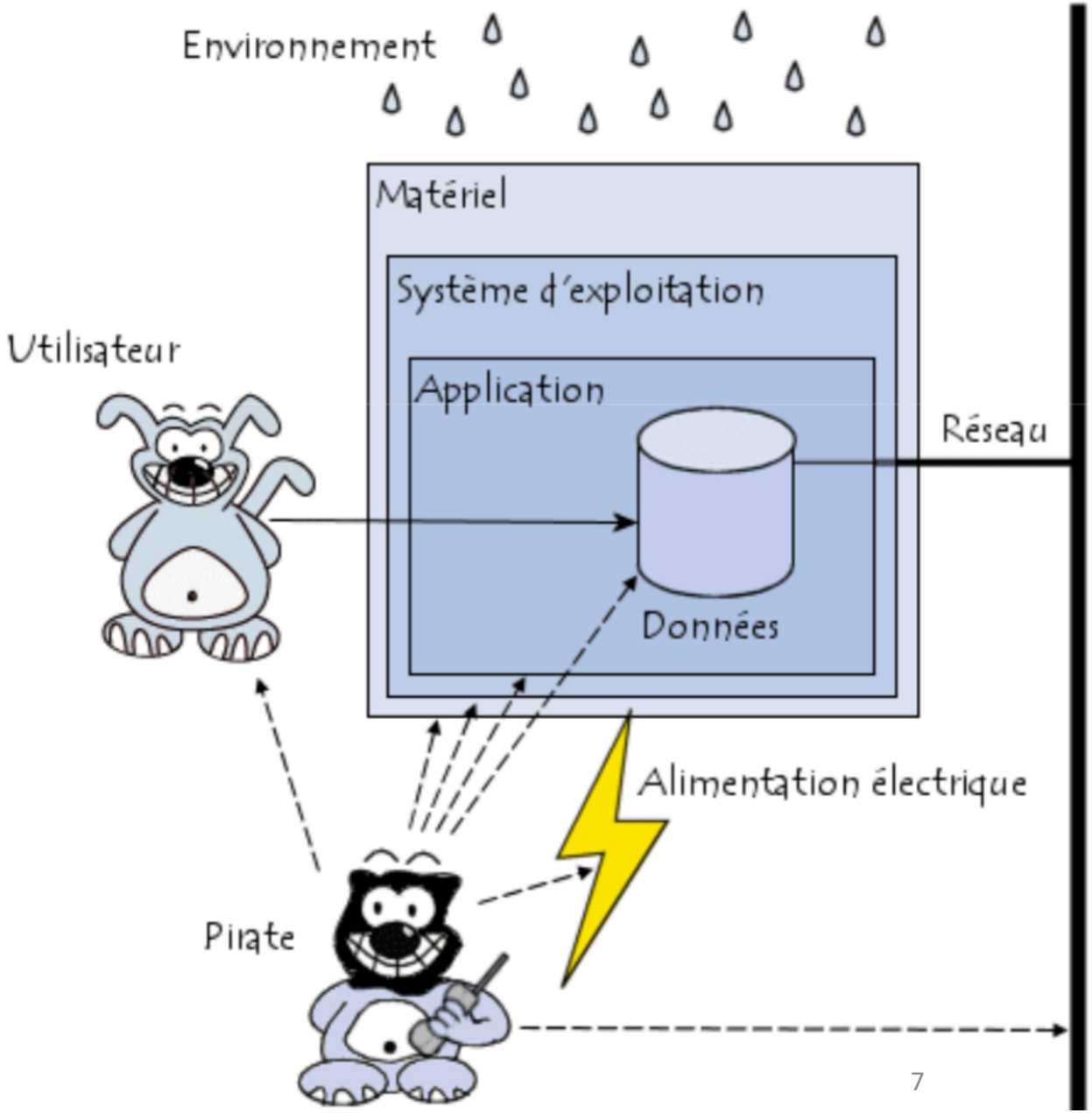
- ✓ Obtenir un accès au système
- ✓ Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles
- ✓ Collecter des informations personnelles sur un utilisateur
- ✓ Récupérer des données bancaires ;
- ✓ S'informer sur l'organisation (entreprise de l'utilisateur, etc.)
- ✓ Troubler le bon fonctionnement d'un service
- ✓ Utiliser le système de l'utilisateur comme « rebond » pour une attaque
- ✓ Utiliser les ressources du système de l'utilisateur, notamment lorsque
- ✓ Le réseau sur lequel il est situé possède une bande passante élevée

Attaquer pour le bien ou le mal

Intrusion (attaque)

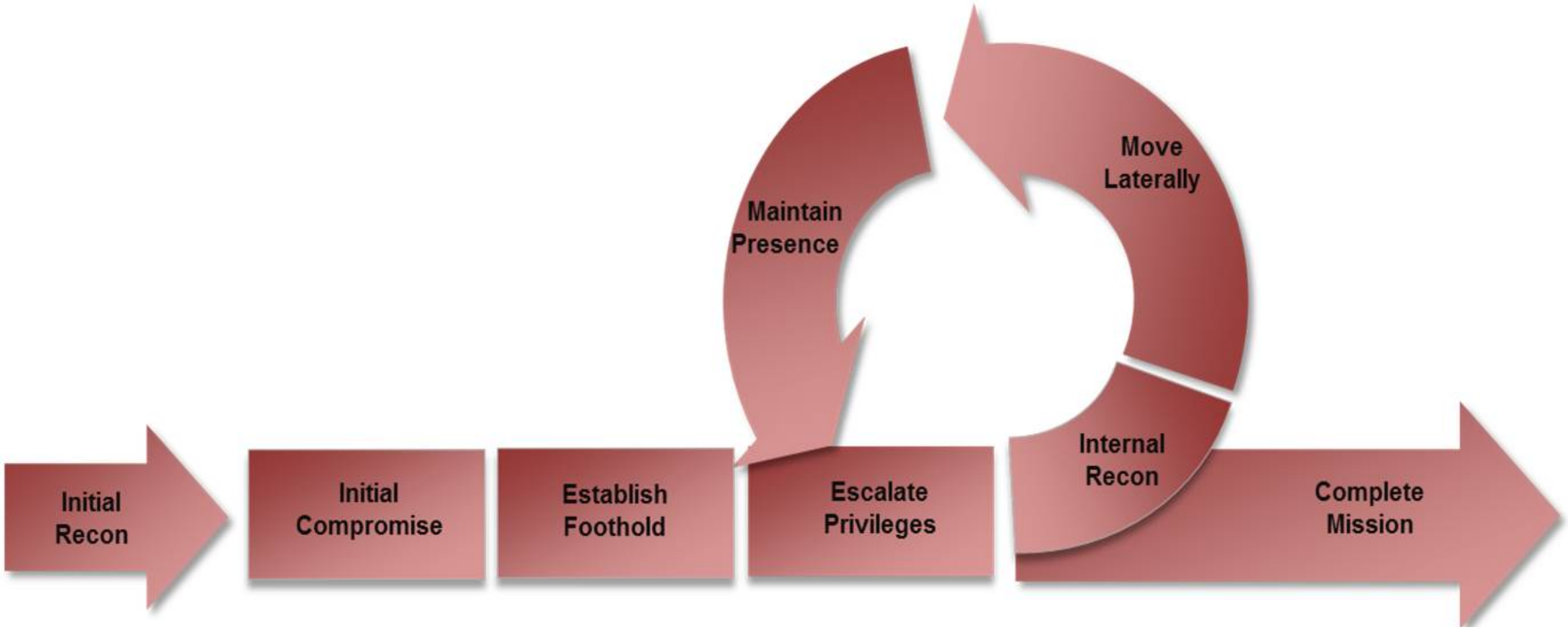
Quoi attaquer?

- ✓ Les attaques peuvent intervenir à chaque maillon de la chaine des composantes du système d'information, pour peu qu'il existe une vulnérabilité exploitable.



Intrusion (attaque)

le cycle de vie d'une intrusion :



https://www.fireeye.com/services.html

Intrusion (attaque)

le cycle de vie d'une intrusion :

1. Reconnaissance initiale

- ✓ Permet une analyse superficielle permettant d'avoir des informations générales sur la victime et/ou le système
- ✓ Maltego, Google search, archive.org..etc.

2. Compromis initial

- ✓ Exécuter des codes malicieux sur le système cible permettant de lancer l'attaque comme l'installation d'un sniffer ou questionnaire assurant l'ingénierie sociale

Intrusion (attaque)

le cycle de vie d'une intrusion :

3. Établir une implantation

- ✓ L'attaquant s'assure qu'il conserve un contrôle continu sur le système. En générale, l'attaquant prend pied en installant une porte dérobée persistante ou en téléchargeant des utilitaires ou des logiciels malveillants supplémentaires sur le système victime.

4. Contrôle des privilèges

- ✓ Pour avoir plus de contrôle, les attaquants augmentent souvent leurs privilèges par le vidage du hachage de mot de passe, la journalisation des frappes / des informations d'identification, l'obtention de certificats PKI, l'exploitation des privilèges détenus par une application ou l'exploitation d'un logiciel vulnérable.

Intrusion (attaque)

le cycle de vie d'une intrusion :

5. Reconnaissance interne

- ✓ L'attaquant commence à exploiter l'environnement du système cible afin d'avoir une analyse en amont permettant d'avoir des détails qui guide l'attaque.

6. Déplacer latéralement

- ✓ L'attaquant à cette étape utilise des utilitaires et exploite des failles d'accès à distant afin de déplacer dans l'environnement du système ce qui permet la découverte et la propagation de l'attaque.

Intrusion (attaque)

le cycle de vie d'une intrusion :

7. Maintenir la présence

- ✓ Afin de maintenir un accès permanent aux systèmes. L'attaquant installe plusieurs portes dérobées ou des canaux cachés permettant des futurs accès.

8. Compléter la mission

- ✓ Après qu'il a atteint son objectif, l'attaquant supprime ses traces d'exécution des différents programmes et commandes dans le système tout en gardant l'accès déterminé dans l'étape précédente.

Intrusion (attaque)

Classification des attques :

1ère classification:

Selon l'origine d'attaque

- ✓ **Attaques internes:** Un employeur copie les fichiers secrets de l'organisme dans son flash disque

- ✓ **Attaques externes:** Un pirate réussit à avoir les mots de passe du caissier de la banque

Intrusion (attaque)

Classification des attques :

2ème classification:

Selon l'objectif visé

- ✓ **Confidentialité:** Un employeur connaître la listes des informations personnelles de ses collègues
- ✓ **L'intégrité:** Un employeur modifie son salaire dans le système
- ✓ **La disponibilité:** Le serveur de site web tombe en panne
- ✓ **L'authenticité:** Un dirigeant envoie un ordre au nom de son directeur aux autres employeurs

Intrusion (attaque)

Classification des attques :

3ème classification:

Selon l'impact de l'attaque

- ✓ **Passives:** Des attaques qui ne causent pas un changement dans le système (vol des mots de passe, lecture des informations …etc.)
- ✓ **Active:** Des attaques qui provoque un changement accidentels ou délibéré au système (arrêt de service, modification des données…etc.)

Intrusion (attaque)

Classification des attques :

4ème classification:

Selon l'emplacement de l'attaque (la cible)

- ✓ **Réseaux:** ne s'exécutent que dans un réseau. Ils ont un large effet (peuvent cibler plusieurs machines à la fois). e. i.: ouverture des sessions à distant (session hijaking)
- ✓ **Système:** s'exécutent dans un système d'exploitation même s'ils sont été transporté à travers un réseau (virus…etc.)
- ✓ **Physique:** visant la sécurité physique du système (voleur casse la porte du l'entreprise).

Intrusion (attaque)

Exercice de rafraichissement :

Classez les attaques suivantes selon les 4 classifications vues précédemment:

1. Inondation du réseau par des paquets vides

2. Un étudiant réussit à modifier sa note lorsque le professeur a laissé son PC allumé à la salle

3. Agent de bureau utilise l'agrément de son chef pour ses justifications d'absence

4. L'affaire juridique entre Apple et Samsung (cas d'expulsion du designer – copie des design)

5. L'affaire juridique entre Apple et Samsung (cas de produit Galaxy)

Intrusion (attaque)

Exercice de rafraichissement :

Attaque	1ère classification	2ème classification	3ème classification	4ème classification
01				
02				
03				
04				
05				

Intrusion (attaque)

Exercice de rafraichissement :

Attaque	1ère classification	2ème classification	3ème classification	4ème classification
01	Les deux	Disponibilité	Active	Réseau
02	Interne	Intégrité	Active	Système
03	Interne	Authenticité	Active	Physique
04	Ce n'est pas une attaque. C'est une vulnérabilité			
05	Externe	Authenticité	Passive	-

Classification des attaquants

Les organisations:

- ✓ Entreprises concurrentes dans le marché (espionnage commercial)
- ✓ Journaux et journalistes

Les script-kiddies:

- ✓ Ne sont pas des vrais attaquants
- ✓ Utilisent les scripts écrits par des vrais pirates afin d'exploiter des attaques réelles (utilisateurs de linux backtrack)

Classification des attaquants

Les menaces internes:

- ✓Son existence dans légale mais ses tâches ne sont pas celles autorisées
- ✓Corruption, ingénierie sociale et points communs

Classification des attaquants

Les crackers:

- ✓Spécialistes dans le craquage des mots de passe et session hijacking
- ✓Utilisent les attaques (par fois même produise de nouvelles techniques) d'accès

Les hackers:

- ✓Les pirates les plus professionnels et des excellents développeurs
- ✓Servent à découvrir de nouvelles failles ainsi que le développement des attaques qui n'existent pas avant
- ✓Mauvaise coté (black hat) et bonne coté (white hat)

Next?

Les malwares:

✓Définition, composition, types

Les attaques réseaux:

✓Déni de service (DOS), phishing, sniffing, social engineering…etc.