

Sécurité des Systèmes d'Information

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

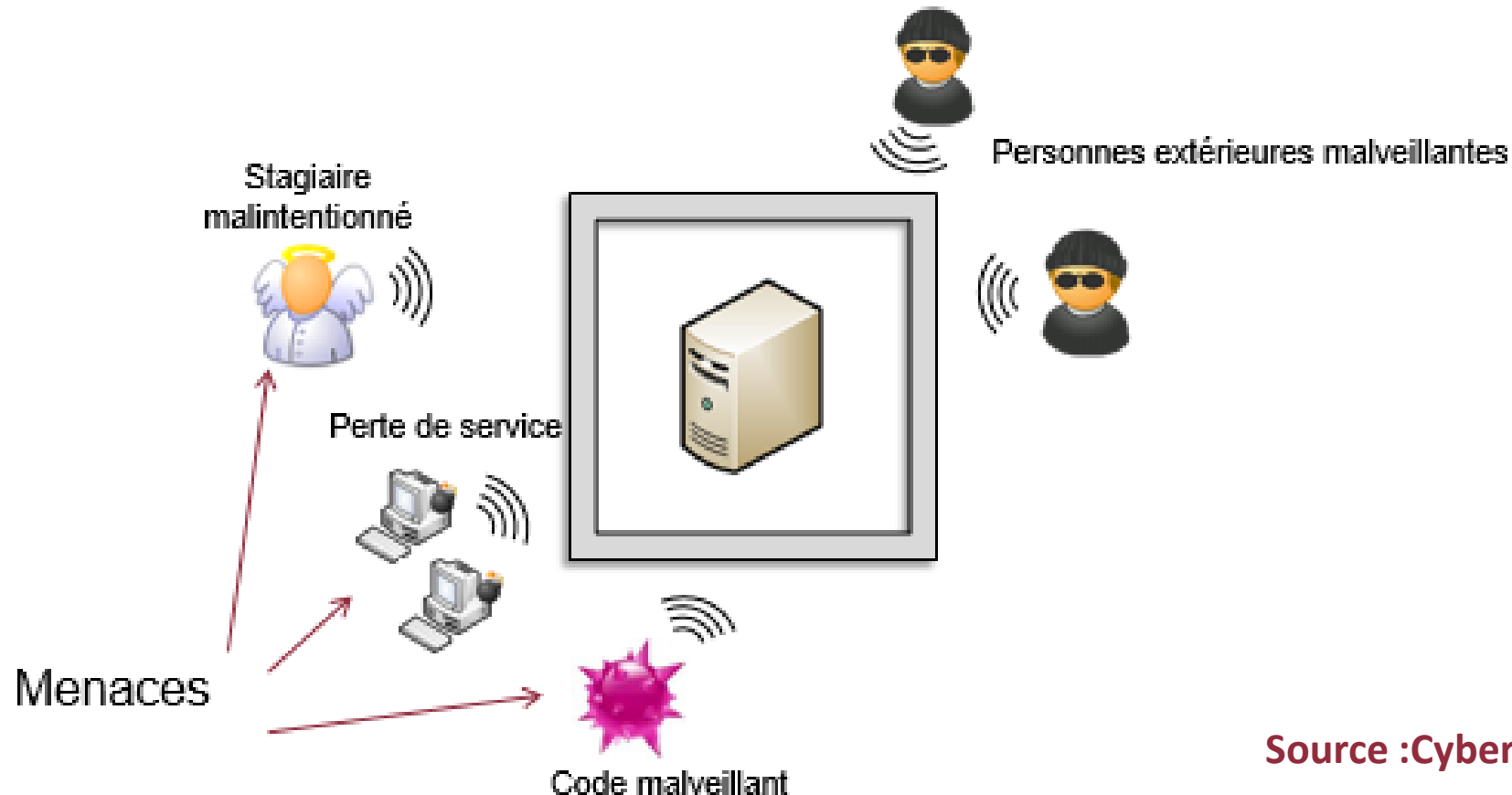
université d'Alger 1 -
Benyoucef Benkhedda

Objectifs du chapitre:

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

Menace:

Un **danger** qui existe dans l'environnement d'un système informatique indépendant de celui-ci.



Source :CyberEdu(NTIC)

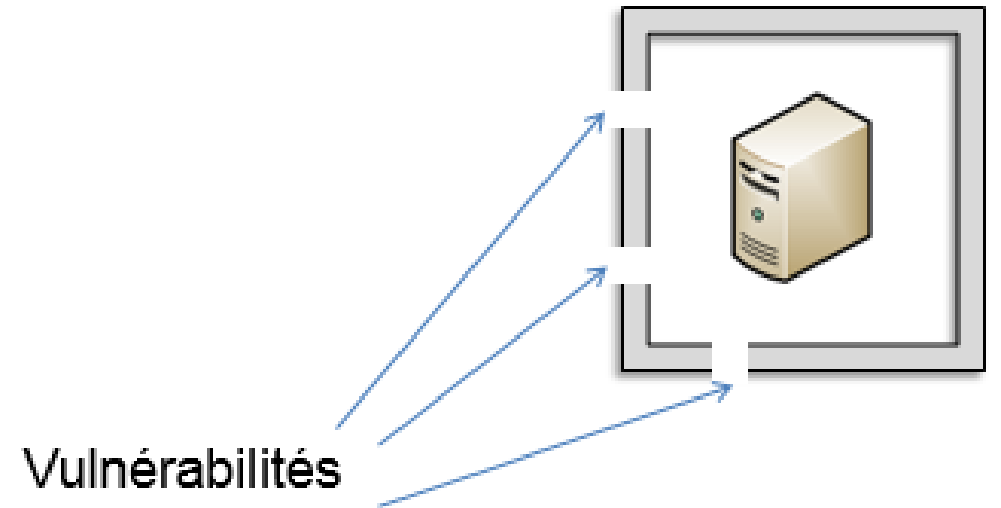
Vulnérabilité (faille):

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/>



Risque :

Un risque est la probabilité qu'une menace particulière puissent exploiter une vulnérabilité donnée du système


Contremesures :

Ce sont les méthodes de contrôle implémenté dans un système informatique pour diminuer ou éliminer le risque

Peuvent être :

- Administratives : charte informatique
- Physique
- Techniques

Exemple :



A user account card with a light blue background. On the left is a dark grey square containing a white person icon. To the right of the icon, the text 'tri' is displayed in a bold font, and 'Compte local' is displayed below it in a smaller font.

- **Votre compte utilisateur n'est pas protégé par un mot de passe**
- **Vous quittez votre bureau pendant 5 minutes**

Exemple :



Le risque augmente

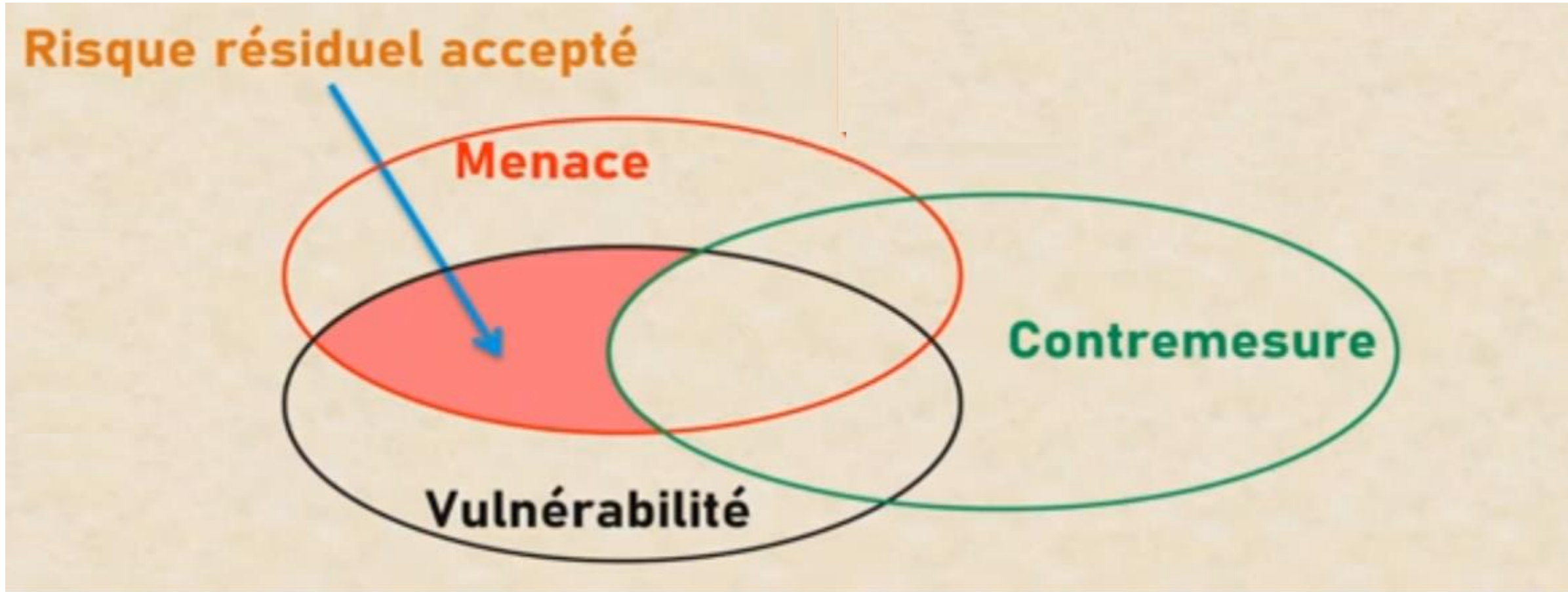


Menace

Vulnérabilités

- Votre compte utilisateur n'est pas protégé par un mot de passe
- Vous quittez votre bureau pendant 5 minutes

Récapitulatif :



Source :Mohamed Qara

Intrusion (attaque)

Action malveillante destinée à porter atteinte à la sécurité d'un bien. Une attaque est **l'exploitation d'une vulnérabilité** au niveau du système informatique à des fins généralement préjudiciables.

Exemple : Contournement de l'authentification dans l'application VNC

L'application VNC permet à un utilisateur de prendre en main sur une machine distance, après qu'il se soit authentifié.

La vulnérabilité décrite dans les planches suivantes est corrigée depuis de nombreuses années. Elle est symptomatique d'une **vulnérabilité dans la conception d'une application** ;

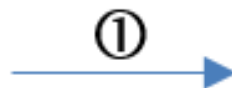
L'application permet en temps normal à un utilisateur de se connecter à distance sur une machine pour y effectuer un « partage de bureau » (i.e. pour travailler à distance sur cette machine) ;


En 2006, il est découvert que cette application – utilisée partout dans le monde depuis de très nombreuses années – présente une vulnérabilité critique : il est possible de se connecter à distance sur cette application **sans avoir besoin de s'authentifier** (i.e. tout utilisateur sur internet peut se connecter à distance sur les systèmes en question) ;

Le diaporama suivant illustre la **vulnérabilité technique** sous-jacente à ce comportement.

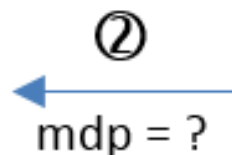
Illustration d'un usage normal de l'application vulnérable

L'utilisateur effectue une demande de connexion au serveur depuis son PC client

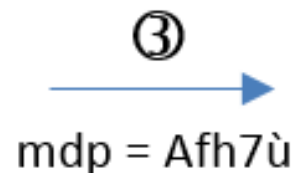


 Description du fonctionnement normal de l'application

Le serveur détermine le mode d'authentification (*aucune authentification, mot de passe, certificat, etc.*) et envoie cette demande d'authentification à l'utilisateur demandeur



L'utilisateur s'authentifie selon la méthode choisie par le serveur



Le serveur valide l'authentification (si elle est correcte) et autorise donc la connexion

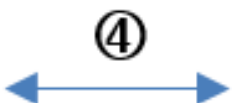
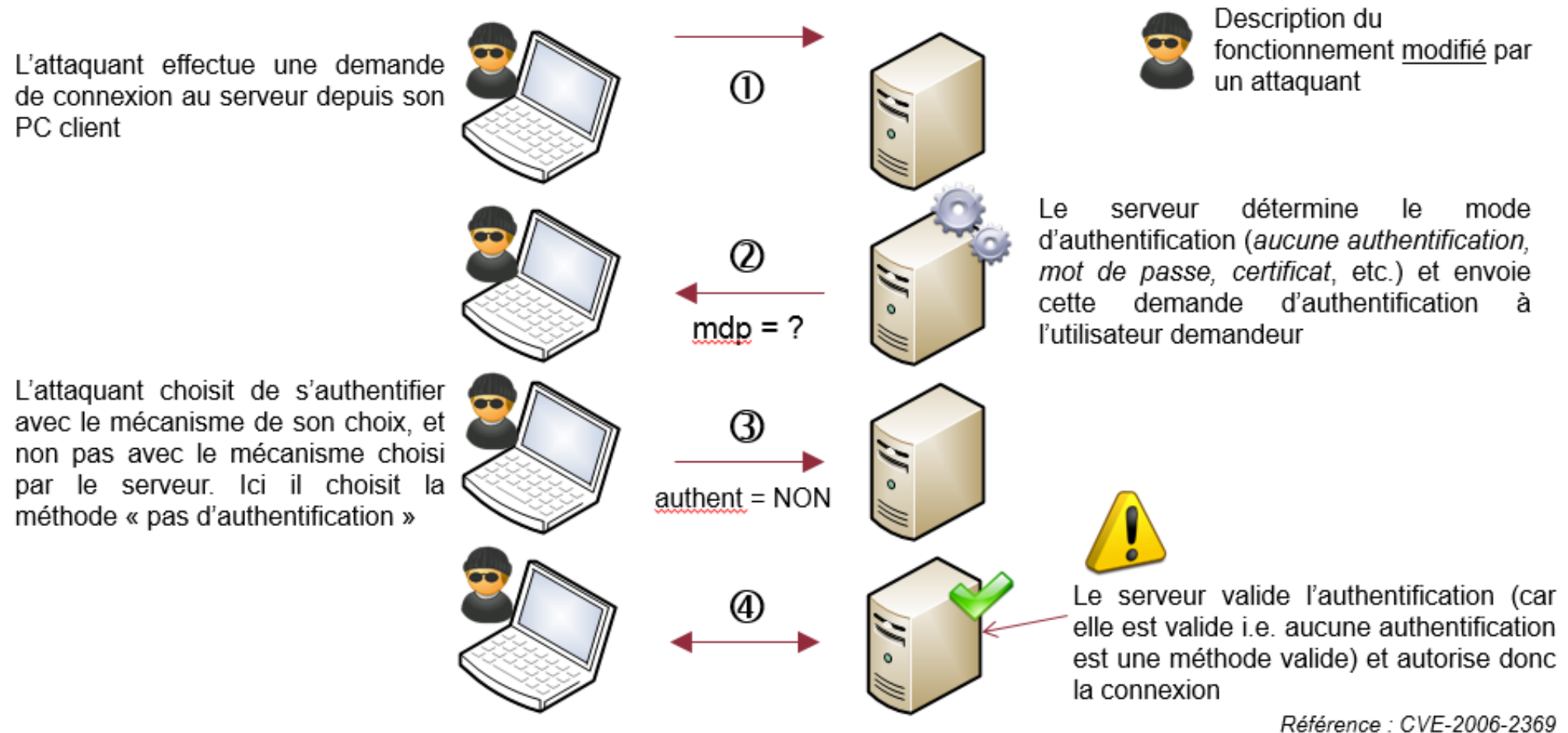


Illustration de l'exploitation de la vulnérabilité présente dans l'application



La vulnérabilité se situe ici : le serveur ne vérifie pas que le type d'authentification retourné par le client correspond à celui demandé. A la place, il vérifie simplement que l'authentification est correcte (et « **authent = NON** » est effectivement une authentification qui est toujours correcte)

Intrusion (attaque)

Pourquoi attaquer?

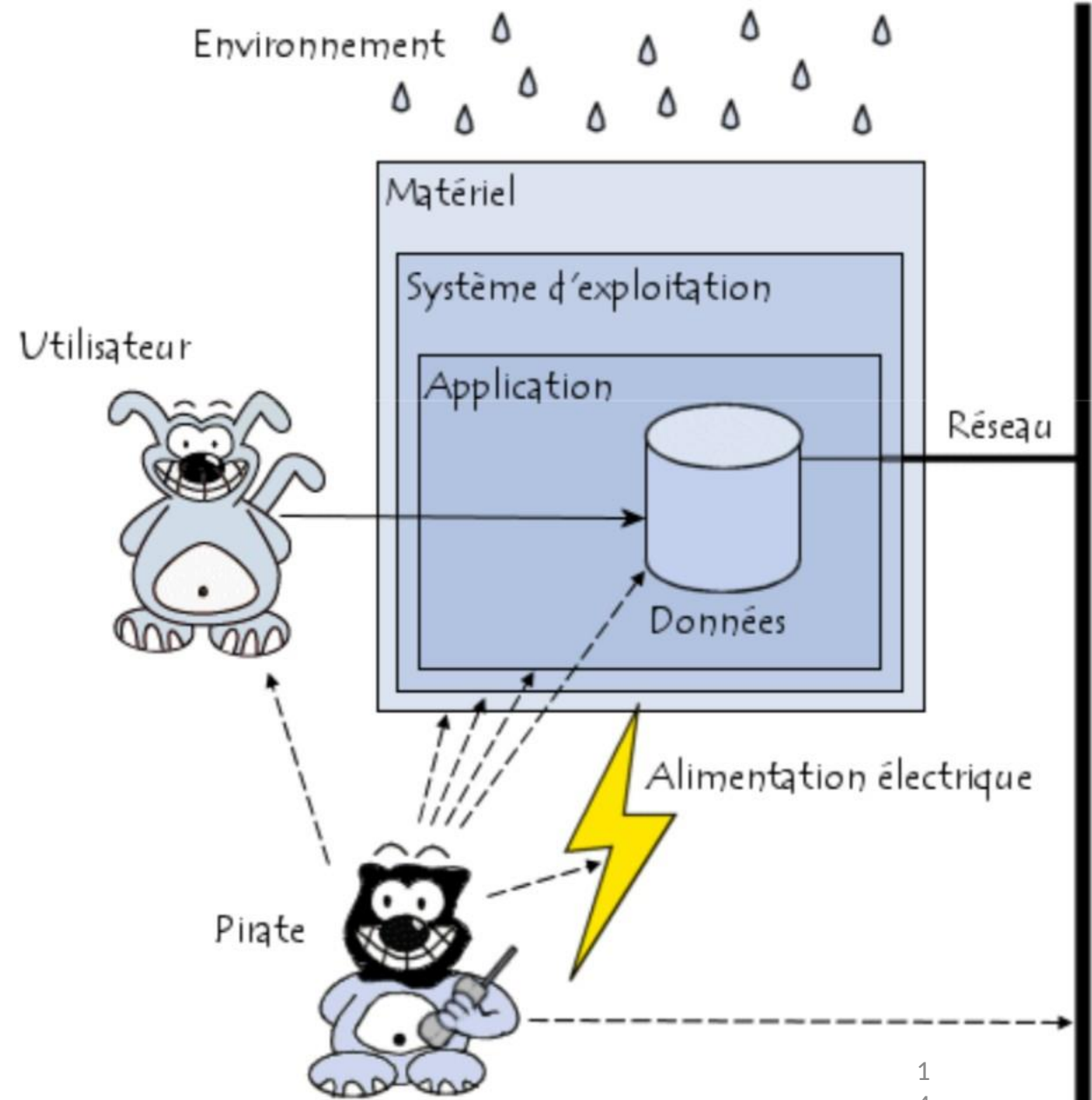
- ✓ Obtenir un accès au système
- ✓ Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles
- ✓ Collecter des informations personnelles sur un utilisateur
- ✓ Récupérer des données bancaires ;
- ✓ S'informer sur l'organisation (entreprise de l'utilisateur, etc.)
- ✓ 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 chaîne des composants du système d'information, **pour peu qu'il existe une vulnérabilité exploitable.**



Intrusion (attaque)

Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.

Ainsi, tout le travail des experts sécurité consiste à s'assurer que le S.I. ne possède aucune vulnérabilité.

Dans la réalité, l'objectif est en fait d'être en mesure de maîtriser ces vulnérabilités plutôt que de viser un objectif 0 inatteignable.

Source :CyberEdu(NTIC)

Exemple d'attaque

Source :CyberEdu(NTIC)



Copé, Hortefaux, Dassault... leurs messageries Orange piratées

par Emilien Ercolani, le 07 mai 2013 15:04 ★★★★★

Les messageries des téléphones portables de plusieurs personnalités politiques (JF Copé, B Hortefaux) ou industrielles (la famille Dassault) ont été piratées plusieurs semaines durant. Des plaintes ont été déposées, alors qu'Orange a lancé une enquête interne.

Publié le 13 avril 2014 à 12h24 | Mis à jour le 13 avril 2014 à 12h24

Le centre allemand de recherche spatiale cible d'une cyberattaque

Agence France-Presse

Le centre allemand de recherche aéronautique et spatiale (DLR) a été la cible il y a quelques mois d'une cyberattaque présumée par un service de renseignements étranger, affirme le magazine Der Spiegel dimanche.

Actualités > Société

Une panne réseau a cloué au sol les avions d'American Airlines

Près de 670 vols ont été annulés hier, en raison d'un problème d'accès au système de réservation. La compagnie s'est appuyée sur les réseaux sociaux pour informer ses clients.



Gilbert Collomb, avec AFP | D1net | le 17/04/13 à 15h23 | Partager un avis

Twitter 2 0

Panne informatique à l'hôpital de

En l'espace de deux jours, mercredi et jeudi, l'accueil aux urgences de a été très perturbé. Il a fallu diriger les patients vers d'autres hôpitaux.

Publié le 10.01.2009

Des machines à sous vidées à cause d'une faille informatique

Le Monde 9 | 10.04.2014 à 09h09 | Mis à jour le 10.04.2014 à 10h40

Recommandé

5 images

5 classes

5 tags

5 partages

Partager



Ukraine : le mystérieux virus Snake infecte les ordinateurs du gouvernement

Publié le 08.03.2014, 16h50 | Mise à jour : 17h23

Recommandé

12 personnes le recommandent

Recommander

Twitter

44

5+1

Share

5

5

5

5



Exemple d'attaque

Source :CyberEdu(NTIC)



Bug informatique à La Poste : "Tout est rentré dans l'ordre"



par Caroline Piquet
le 30 juillet 2013 à 15h50, mis à jour le 30 juillet 2013 à 18h59.

A la suite d'une panne informatique, les opérations de prélèvements et de virements bancaires accusent un retard de 24 heures. Ce mardi, les clients ne pouvaient accéder à leurs soldes sur Internet et il leur était impossible de retirer de l'argent aux distributeurs automatiques.

Hacker un pacemaker, c'est possible et c'est dangereux

© 12 - vendredi 10 octobre 2012 - Par Adrien Moe - Source : France Info



Une panne informatique paralyse Wall Street pendant 3 heures

Edité par MYTF4News avec AEP
le 23 août 2013 à 06h50, mis à jour le 23 août 2013 à 07h02.

Help! My fridge is full of spam and so is my router, set-top box and console
Security company says it discovered spam and phishing campaign run over Christmas, which involved internet fridge

Charles Arthur
Follow @charlesarthur Follow @guardiantech
theguardian.com, Tuesday 21 January 2014 11:40 GMT
Jump to comments (18)



Gibraltar: un incendie interrompt des services de paris en ligne

AFP, 2004 23:01 CET



Un avion espion « plante » le système informatique d'un aéroport

Exemple d'attaque

Source :CyberEdu(NTIC)

Sony Pictures Entertainment



« Si vous n'obéissez pas, nous publierons au monde les informations suivantes ». Ce message était affiché sur plusieurs ordinateurs de Sony Pictures Entertainment le 24 nov 2014

- GOP pour Guardian of Peace
- Des données internes ont été publiées contenant :
 - les numéros de sécurité sociale et les numérisations de passeport appartenant aux acteurs et directeurs.
 - des mots de passe internes
 - des scripts non publiés
 - des plans marketing
 - des données légales et financières
 - et 4 films entiers inédits
- La probabilité de vol d'identité est très forte désormais pour les personnes dont les informations ont été publiées.
- Les studios concurrents de Sony, ont une visibilité sur les plans stratégiques de Sony.

La source de l'attaque reste à déterminer.
La Corée du Nord est soupçonnée d'être à l'origine de l'attaque.

Intrusion (attaque)

Classification des attques :

1^{ère} 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:

2^{ème} classification:

Selon l'objectif visé

- ✓ **Confidentialité:** Un employeur connaît la liste 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 employés

Intrusion (attaque)

Classification des attques :

3^{ème} 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 :

4^{ème} 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 hijacking)
- ✓ **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 de 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 est légale mais ses tâches ne sont pas autorisées
- ✓ Corruption, ingénierie sociale et points communs

Classification des attaquants

Les crackers:

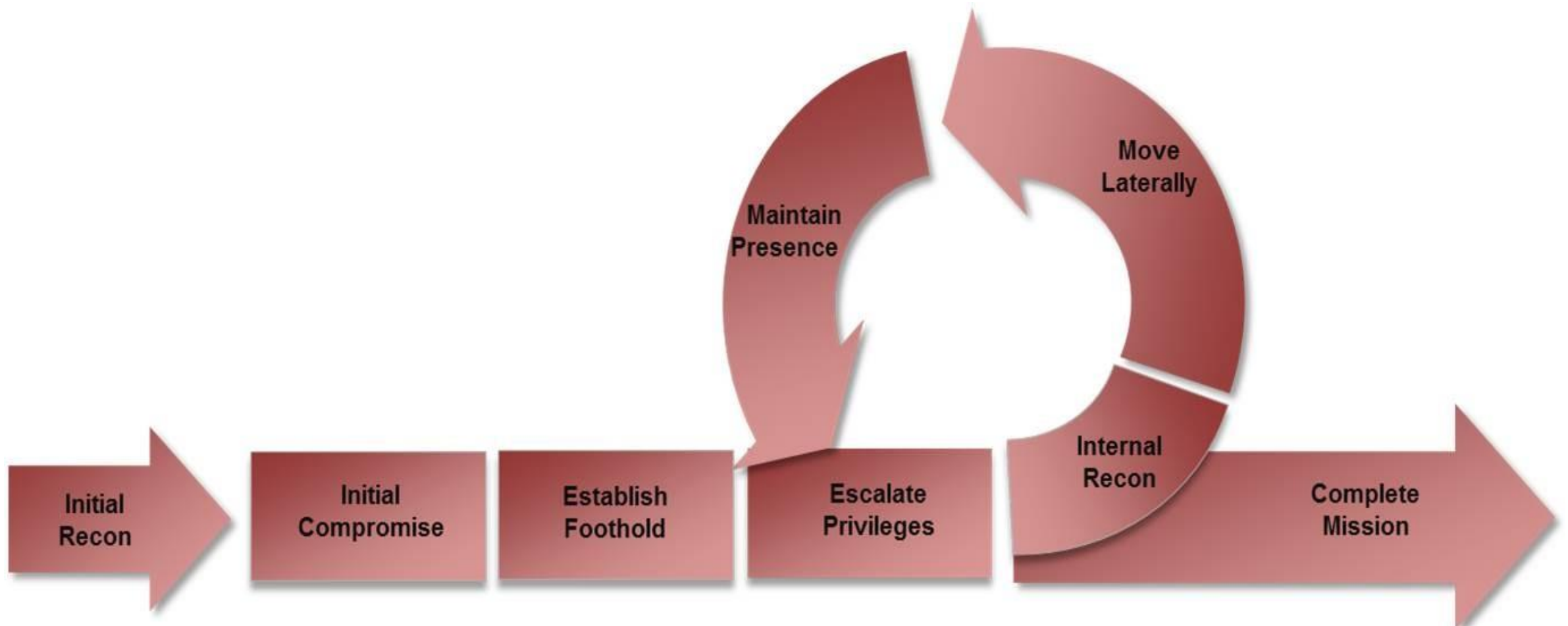
- ✓ Spécialistes dans le craquage des mots de passe et session hijacking
- ✓ Utilisent les attaques (par fois même produise de nouvelles techniques) d'accès

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)

Intrusion (attaque)

le cycle de vie d'une intrusion :



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.

Next?

Les malwares:

- ✓ Définition, composition, types

Les attaques réseaux:

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