Université Mohammed V de Rabat
Ecole Supérieure de Technologie de Salé

Sécurité des données

Pr Rachid ALAOUI

Plan

1- Initiation à la sécurité Informatique

2- Algorithmes de Cryptographies

3- Sécurité des applications

4- Sécurité des bases de données

5- Sécurité Réseaux

6- Introduction à la sécurité Cloud

Université Mohammed V de Rabat
Ecole Supérieure de Technologie de Salé

Chap 1

Initiation à la sécurité Informatique

Pr R.ALAOUI

Exigences d'un projet informatique

- Exigences fonctionnelles:
  - Une application est créée pour répondre , tout d'abord, aux besoins fonctionnels des entreprises.
- Exigences Techniques :
  - Les performances:
    - Temps de réponse
    - Haute disponibilité et tolérance aux pannes
    - Eviter le problème de montée en charge
      Recherche et élimination des goulots d'étranglement
  - La maintenance:
    - Une application doit évoluer dans le temps.
    - Doit être fermée à la modification et ouverte à l'extension
  - Sécurité
  - Portabilité
  - Distribution
  - Capacité de communiquer avec d'autres applications distantes.
  - Capacité de fournir le service à différents type de clients (Desk TOP, Mobile, SMS, http…)
  - …..
  - Coût du logiciel

Introduction

Les exigences de la sécurité de l'information au sein des organisation sont conduit au besoin d'outils automatisés pour protéger fichiers et autres informations.

Ce besoin est accentué pour un **système accessible via :**
un téléphone public
un **réseau de données**

Des changement majeurs affectés à **la sécurité** par l'introduction de **systèmes distribués** et l'utilisation de réseaux et dispositifs de communication pour transporter des données entre un terminal utilisateur et un ordinateur, et entre ordinateurs.

Problèmes de sécurité (1)

- **Internet** :
  - confidentialité
  - anonymat
  - authentification (s'agit-il bien du site de ma banque ?)

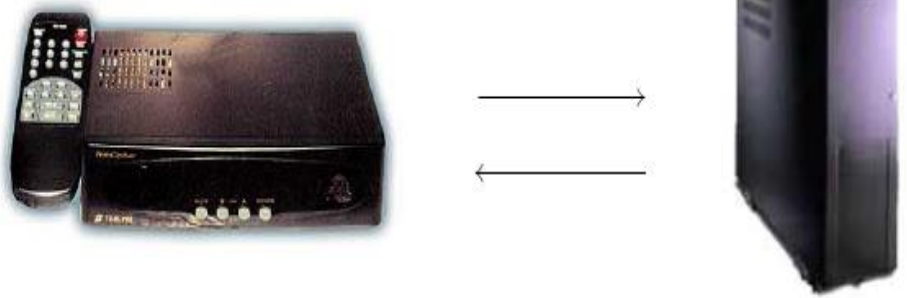
- **Signature électronique:** mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier.

  - vérifiable
  - authentique
  - non-répudiation (je n'ai jamais signé ce texte...)

En pratique, l'essentiel des procédures de signature numérique existantes s'appuie sur la **cryptographie asymétrique**

Problèmes de sécurité (2)

- **Paiement par carte bleue (via dispositif)**
  - Est-ce qu'il s'agit d'une vraie carte ?
  - Est-ce que le montant débité sera égal au montant crédité ?
  - Est-ce que le code secret est bien protégé ?
- **Décodeur, Vérification de l'abonné**
  - Impossibilité de retransmettre les données décodées à une tierce personne
  - Mise à jour de l'abonnement



Problèmes de sécurité (3)

- **Porte monnaie électronique**
  - Pas de création de fausse monnaie
  - Pas de création de faux porte-monnaie

- **Base de données sécurisée**
  - Seules les personnes habilitées ont accès à la vue partielle à laquelle elles ont droit
  - Les données peuvent être échangées entre un médecin, un laboratoire, un hôpital
  - Mise à jour possible des données

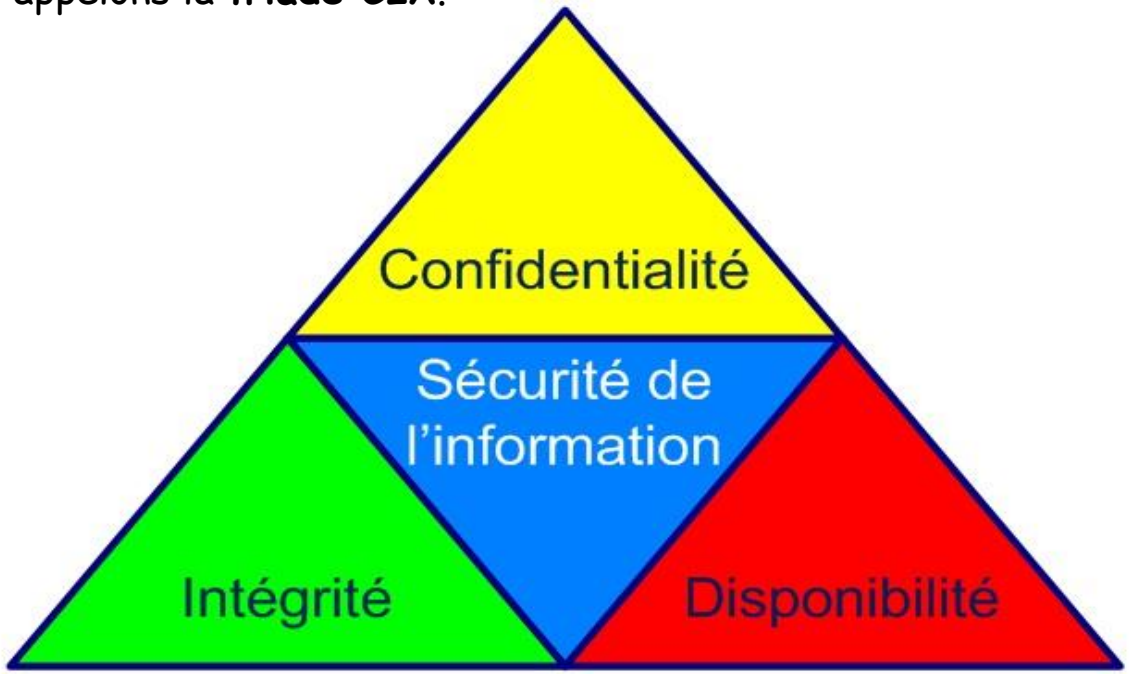
Introduction

La sécurité est une préoccupation majeure pour les entreprises et les organisations de toutes tailles, dans tous les secteurs.

La sécurité de l'information est un ensemble:
- de processus,
- d'outils,
- de politiques et
- de systèmes mis en œuvre pour se protéger contre les menaces internes et externes qui peuvent endommager ou perturber les actifs informationnels.

Sécurité de l'information

Les principes fondamentaux de la sécurité informatique sont la
Confidentialité,
Disponibilité
Intégrité.
Ces principes constituent ce que nous appelons la **triade CIA**.

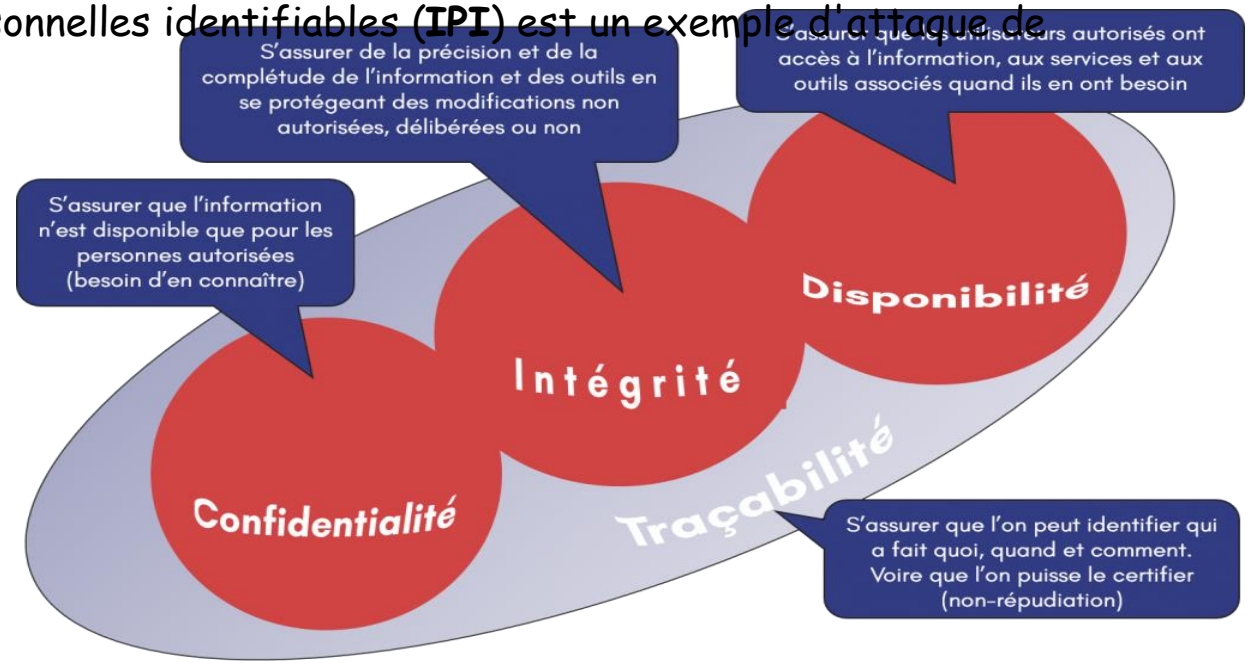


Confidentialité

La confidentialité implique que toutes les informations et données ne sont accessibles qu'aux personnes autorisées à y avoir accès.

Il est important de s'assurer que les informations ne seront pas divulguées par des parties non autorisées.

Le vol d'informations personnelles identifiables (**IPI**) est un exemple d'attaque de confidentialité.

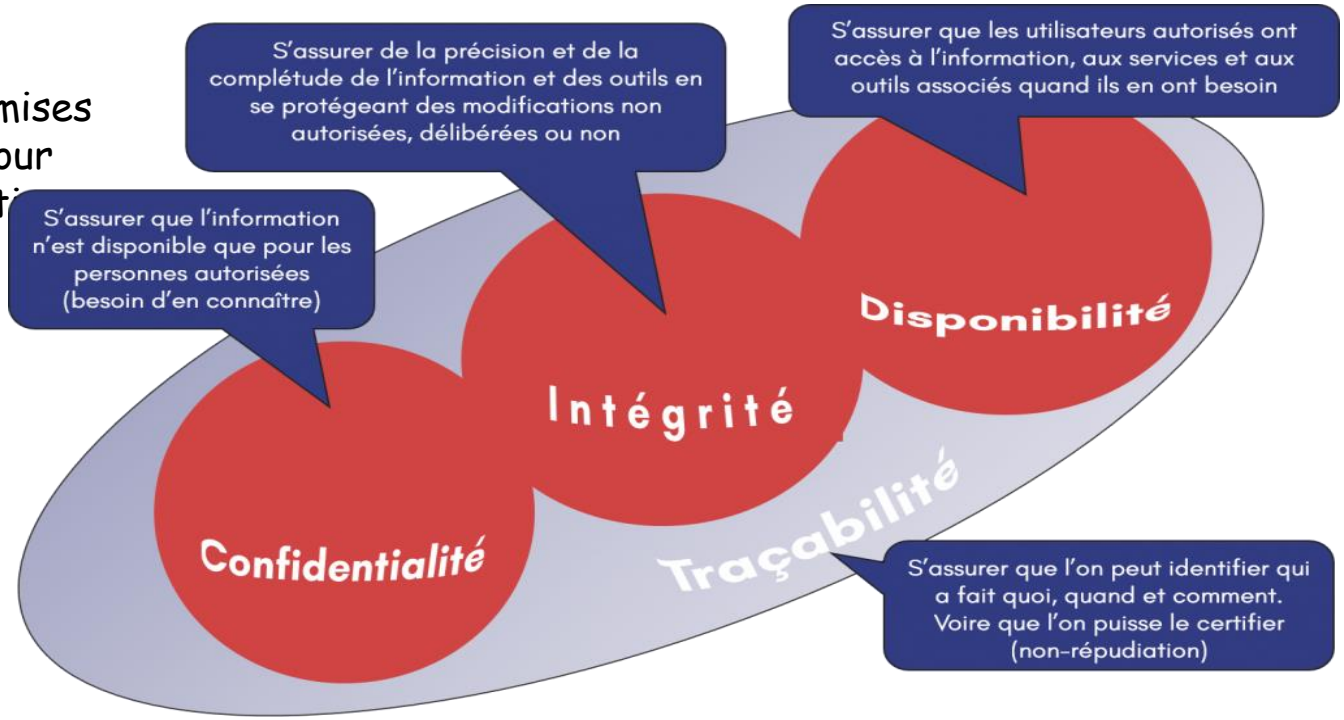


Intégrité

L'objectif de l'intégrité est de protéger les informations contre toute modification non autorisée.

C'est garantir la **fiabilité** des données.
Cela signifie que les données doivent être **cohérentes**, **exactes** et **fiables** à chaque étape du processus d'information.

Certaines méthodes de protection doivent être mises en place et disponibles pour détecter toute modificati des données.

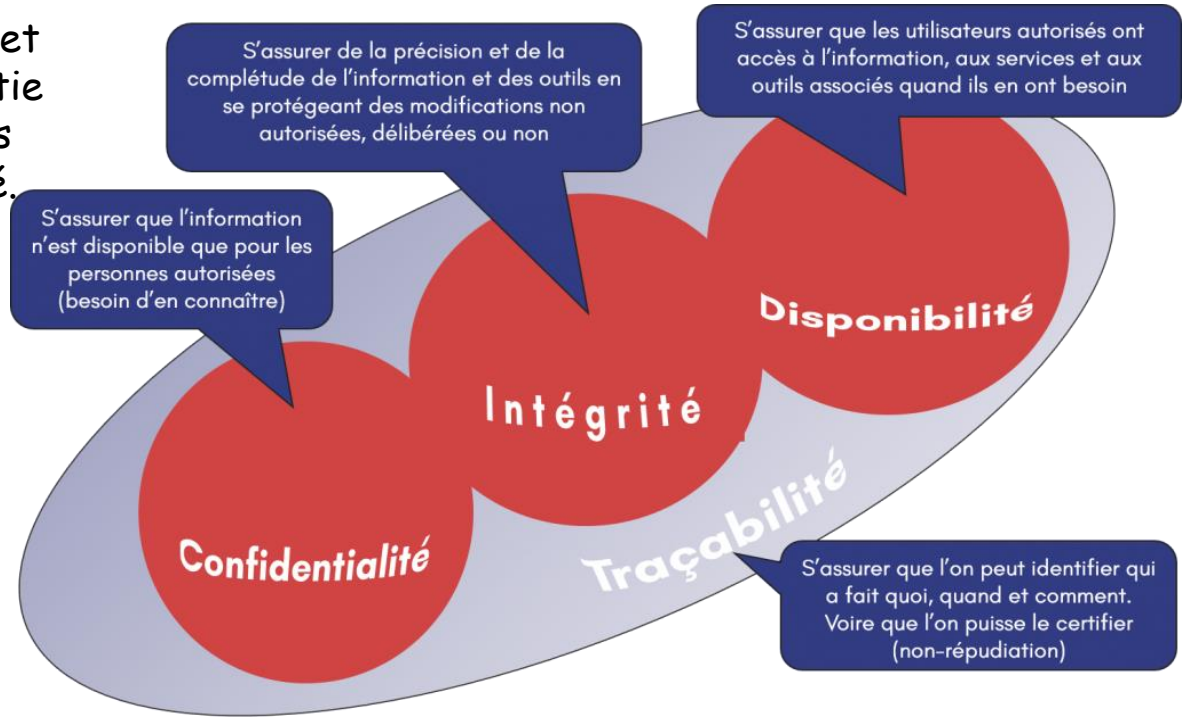


Disponibilité

La disponibilité vise à garantir que les informations sont disponibles pour les utilisateurs autorisés lorsqu'ils en ont besoin.

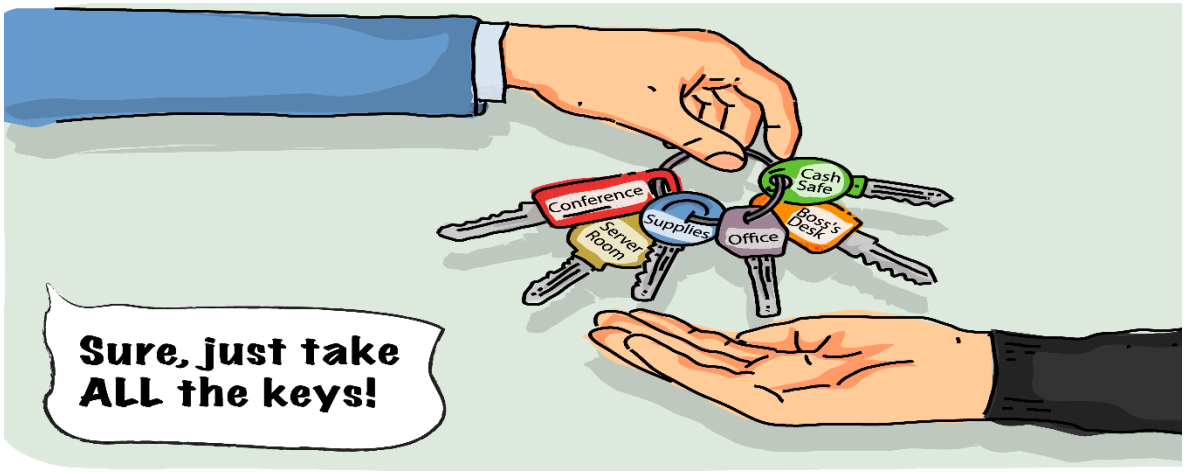
Le **déni de service (DoS)** est un exemple d'attaque de disponibilité.

Les **clusters à haute disponibilité** et les **copies de sauvegarde** font partie des systèmes d'atténuation utilisés contre les attaques de disponibilité.



Le moins de privilèges et le besoin de savoir

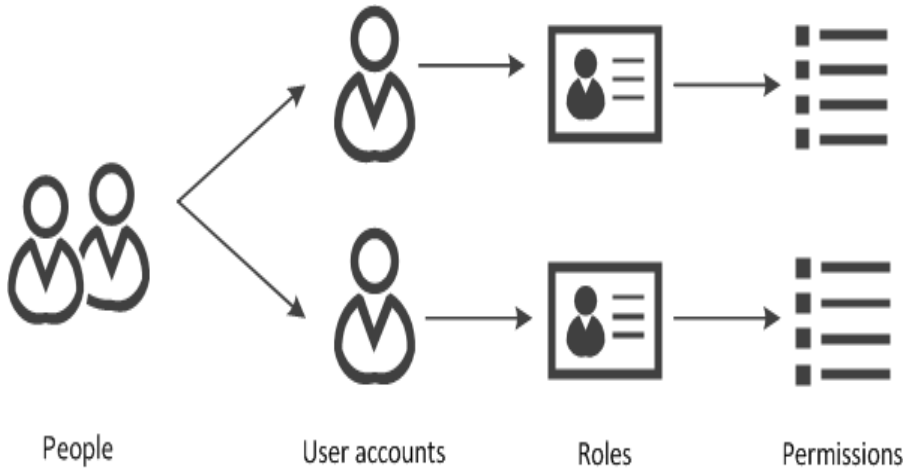
Le principe du **moindre privilège** et du **besoin de savoir** décrit **le fait** que les **utilisateurs autorisés** doivent **bénéficier du minimum d'accès** et **d'autorisations** dans le **cadre de leur travail**.



Le **besoin de savoir** signifie que **l'utilisateur** doit **avoir une raison légitime** pour **accéder aux informations**.

Principe du moindre privilège (Least Privilege)

Le principe du moindre privilège stipule qu'un utilisateur, un système, ou un processus ne doit disposer que des privilèges nécessaires pour accomplir ses tâches spécifiques, et rien de plus.



Pourquoi appliquer le moindre privilège ?

Réduction de la surface d'attaque :

Moins un utilisateur ou un processus a de droits, moins il peut causer de dommages en cas de compromission.

Limitation des erreurs humaines :

Moins de privilèges réduisent les risques d'erreurs accidentelles.

Isolation des risques :

Si un compte est compromis, l'attaquant aura accès uniquement aux ressources autorisées à ce compte.

Exemples :

• Un utilisateur dans une organisation doit **lire** les fichiers financiers mais n'a pas besoin de **modifier** ces fichiers.
Ses privilèges seront limités à la lecture seule.

• Un administrateur de base de données n'a accès qu'aux **outils de gestion des bases de données** et non à l'ensemble du système.

• Une application n'a le droit que d'accéder à un répertoire précis pour y sauvegarder des fichiers.

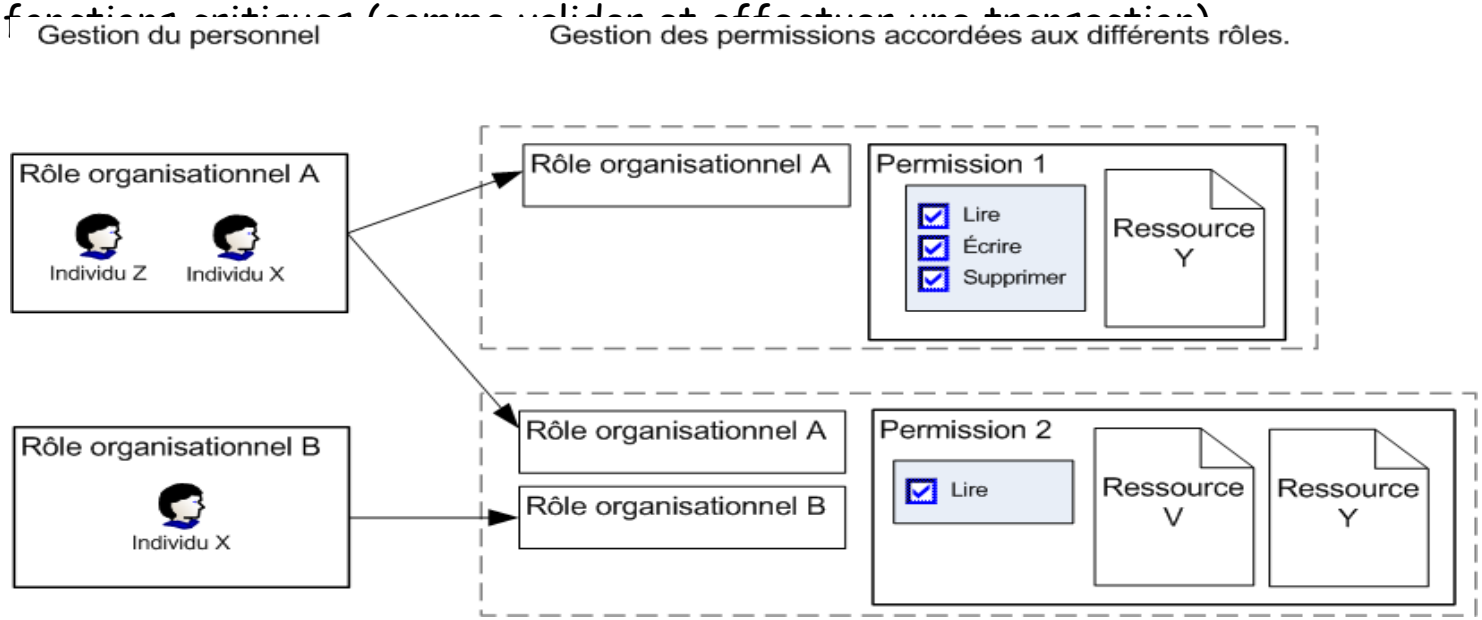
Mise en œuvre de moindre privilège :

• Attribuer des **rôles et des permissions spécifiques** selon les responsabilités.

• Utiliser des **politiques RBAC (Role-Based Access Control)** ou **ABAC (Attribute-Based Access Control)**.

• Surveiller régulièrement les permissions et **révoquer les accès inutiles**.

• Appliquer le **principe de séparation des privilèges** : par exemple, un utilisateur ne peut pas combiner des fonctions critiques (comme valider et effectuer une transaction).



Principe du besoin de savoir (Need to Know)

Le **principe du besoin de savoir** stipule qu'une personne ou un système ne peut avoir accès **qu'aux informations nécessaires** à l'accomplissement de sa mission ou de ses tâches spécifiques.

Pourquoi appliquer le besoin de savoir ?

- **Protection des données sensibles** :
Empêche la divulgation non autorisée d'informations.
- **Confidentialité** :
Limite les informations disponibles à ceux qui ont une **raison légitime** d'y accéder.
- **Réduction des fuites d'information** :
Même en cas de compromission, l'accès aux données est limité.

Exemples :

- Un employé du département des **ressources humaines** n'a besoin d'accéder qu'aux informations liées aux **salaires** et **contrats** des employés, pas aux données financières globales de l'entreprise.
- Un développeur qui travaille sur une **application partielle** n'aura accès qu'au code de cette partie et pas à l'intégralité du projet.
- Un militaire ou un employé d'une agence gouvernementale n'accède qu'à des informations classifiées spécifiques à sa mission.

Mise en œuvre de Besoin de savoir :

• Classifier les données en fonction de leur **sensibilité** (publique, interne, confidentielle, secrète).

• Attribuer l'accès aux données uniquement à ceux qui ont un **besoin professionnel**.

• Utiliser des **mécanismes de chiffrement** pour sécuriser les informations et assurer qu'elles ne sont accessibles qu'aux destinataires autorisés.

• Appliquer des politiques de **contrôle d'accès granulaire**.

Combinaison des deux principes le Moindre privilège et le Besoin de savoir

Ces deux principes sont souvent appliqués ensemble pour renforcer la sécurité :

1. **Moindre privilège** : Contrôle l'accès aux **ressources** et aux **actions** (exécution, lecture, écriture, suppression).

2. **Besoin de savoir** : Contrôle l'accès aux **informations** et **données sensibles**.

Exemple pratique :

Dans une entreprise :

Un **comptable** a le droit d'accéder aux systèmes financiers (**besoin de savoir**) mais ne peut **modifier que certaines transactions** selon ses droits d'accès (**moindre privilège**).

Analyse des risques

Le rôle principal d'un professionnel de la **sécurité de l'information** est d'**évaluer les risques** par rapport aux **actifs de l'entreprise** (ressources qui ont besoin de protection) et de **mettre en œuvre** des **contrôles de sécurité** pour se **défendre contre ces risques**.

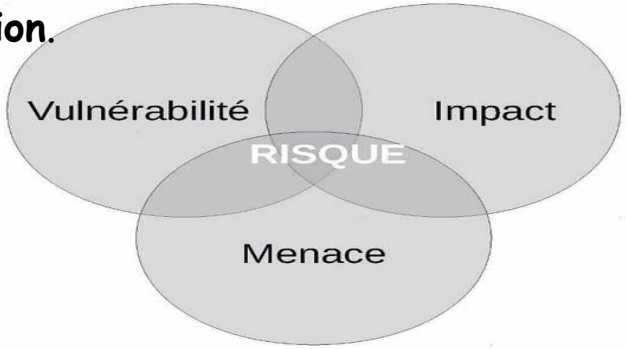
L'analyse des risques est une **compétence** très importante, car un **bon jugement** nous permettra de **sélectionner les meilleurs contrôles de sécurité** et mécanismes de **protection**, y compris le montant des ressources financières nécessaires au déploiement de ces mesures de protection.

Une mauvaise décision coûtera à l'entreprise une **énorme somme d'argent** et, pire encore, **la perte des données des clients**.

L'analyse des risques de sécurité

L'analyse des risques de sécurité est un **processus** crucial pour **identifier et évaluer** les **risques potentiels** pour **les systèmes d'information**,
les **données** et
la **posture de sécurité globale d'une organisation**.

Cela implique **d'analyser**
les vulnérabilités,
les menaces
les impacts potentiels



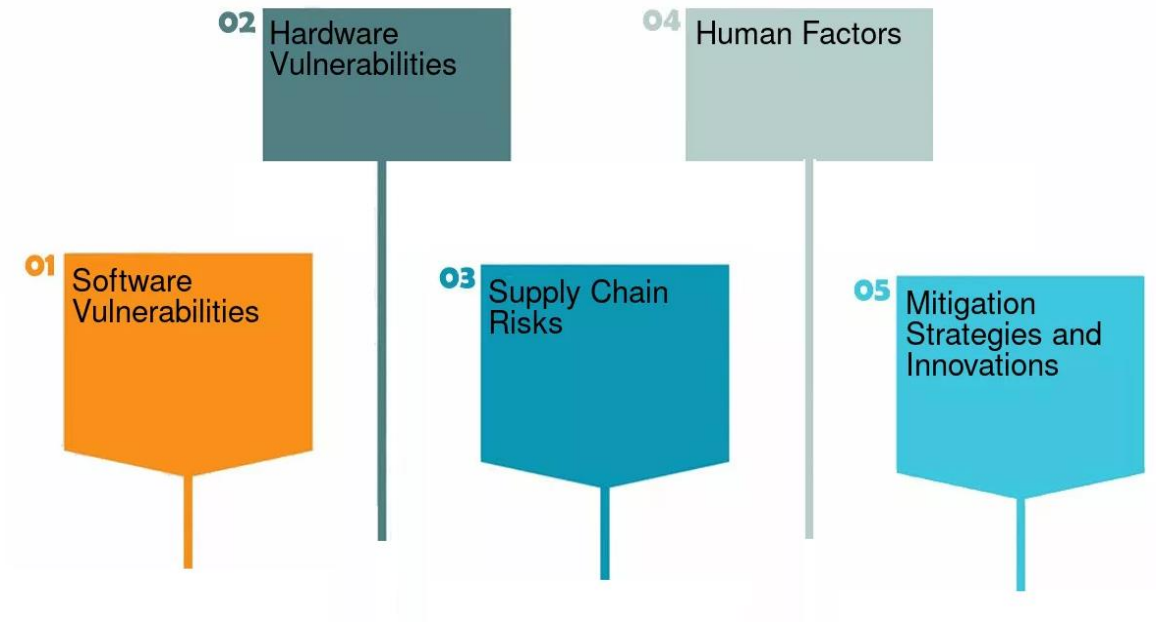
pour déterminer le **niveau de risque** associé à des actifs et des systèmes spécifiques.

1. Identification des vulnérabilités :

la première étape de **l'analyse des risques de sécurité** consiste à **identifier les vulnérabilités** au sein des **systèmes et de l'infrastructure** d'une organisation.

Ces vulnérabilités peuvent exister dans:
- **le matériel,**
- **les logiciels,**
- **les configurations réseau**
- **dans les pratiques du personnel**.

- Les **risques de la chaîne d'approvisionnement** (**Supply Chain Risks**) font référence aux **vulnérabilités** et aux menaces qui émanent des **fournisseurs**, **partenaires** ou **prestataires externes** avec lesquels une organisation collabore.



En identifiant ces faiblesses, les organisations peuvent prendre des mesures proactives pour atténuer les risques avant qu'ils ne soient exploités par des acteurs malveillants.

2. Évaluation des menaces :

Une fois les vulnérabilités identifiées, l'étape suivante consiste à **évaluer les menaces potentielles** qui pourraient les **exploiter**.

Les menaces peuvent provenir de **diverses sources**:
des pirates informatiques,
des menaces internes,
des catastrophes naturelles
des erreurs humaines.

En comprenant les menaces potentielles, les organisations peuvent hiérarchiser leurs mesures de sécurité et allouer efficacement leurs ressources.

3. Estimation des niveaux de risque :

après avoir **identifié les vulnérabilités** et **évalué les menaces**, l'analyse des risques de **sécurité évalue la probabilité** et **l'impact potentiel** d'une attaque ou d'une **faille de sécurité**.

Cette estimation aide les organisations à **comprendre** le **niveau de risque associé à chaque vulnérabilité** et à prioriser leurs efforts en conséquence.

Cela leur permet de se **concentrer sur les vulnérabilités** présentant les **niveaux de risque les plus élevés** et d'**investir des ressources** dans la **sécurisation des actifs critiques**.

Pour évaluer la menace et la vulnérabilité, vous devez attribuer un nombre compris entre 1 et 5, par exemple.
Il est possible d'utiliser une autre plage.

Parfois, nous pouvons ajouter un autre facteur appelé **impact**, qui décrit l'impact du dommage causé.

Dans d'autres cas, il est exprimé sous forme de montant d'argent pour décrire le coût de cet impact. La formule pourrait donc être exprimée comme :
Risque = Menace × Vulnérabilité × Impact.

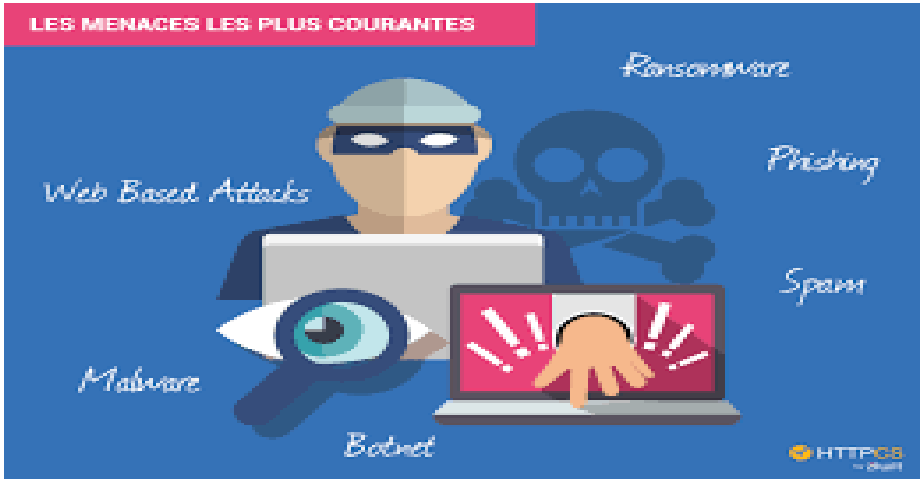
Pour effectuer une analyse des risques qualitative et quantitative, nous pouvons utiliser la **matrice d'analyse des risques** selon la norme **Australie/Nouvelle-Zélande 4360 (AS/NZS 4360)** sur la gestion des risques.

Concepts et phases de piratage informatique

Le **piratage informatique** (ou **hacking**) désigne l'ensemble des actions visant à accéder, manipuler ou perturber des systèmes informatiques, des réseaux ou des données, souvent de manière non autorisée.

Le terme peut couvrir des activités légales (dans le cadre de tests de sécurité) ou illégales (pour voler des informations, causer des dommages, ou obtenir un avantage financier).

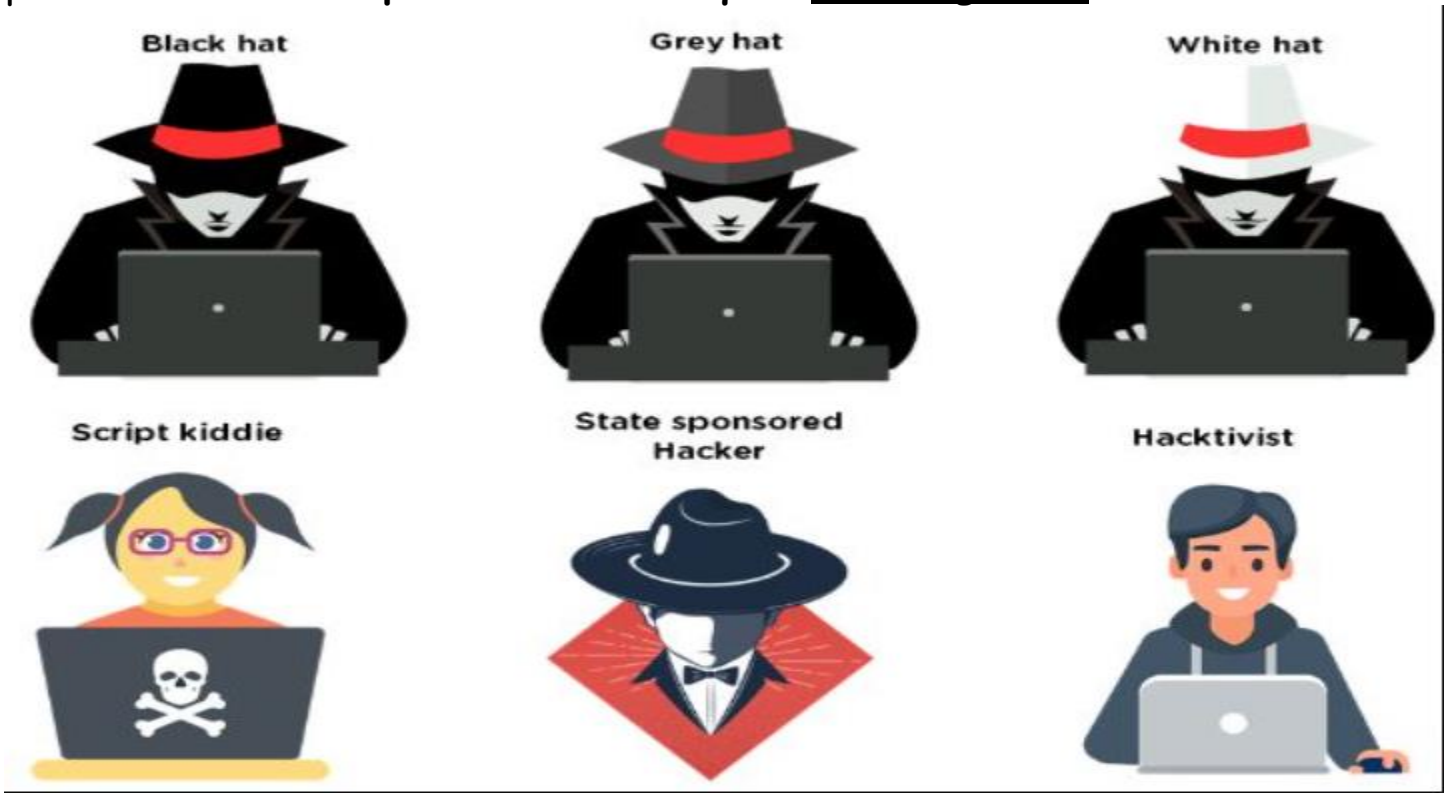
Le **piratage informatique** désigne l'obtention d'un accès non autorisé à un système pour divulguer des données, en exploitant les vulnérabilités du système d'information.



Types de pirates informatiques

Les **pirates informatiques** désignent des **individus ou des groupes** qui utilisent leurs **compétences informatiques** pour **accéder à des informations** à l'aide de **techniques malveillantes**, souvent pour un gain financier.

Nous pouvons **classer les pirates informatiques <u>en catégories</u>** en fonction de leurs intentions :



1- Pirates informatiques black hat :

Si le but du **pirate informatique** est d'**endommager ou de voler** des **informations**

hackers ayant des **intentions malveillantes** qui obtiennent un **accès non autorisé aux réseaux** et **systèmes informatiques**.

Les hackers Black Hat visent à **exploiter les vulnérabilités** de sécurité dans les **logiciels ou les systèmes d'entreprise.** Cela permet souvent d'obtenir un gain financier en incitant les organisations à une rançon ou en vendant des données à des entreprises tierces et à d'autres cybercriminels.

Les hackers Black Hat ont l'intention de voler ou de détruire des données sensibles ou privées, et de perturber ou d'arrêter des réseaux et des sites Web, souvent à des fins financières.

Dans le piratage éthique, un **testeur de sécurité** agit essentiellement **comme** un **hacker**. Il **utilise des outils et des techniques** qu'un hacker utiliserait probablement pour tester la sécurité d'un réseau cible.

La différence est que le **testeur de pénétration est embauché par l'entreprise** pour **tester sa sécurité** et, une fois terminé, révèle à l'équipe de direction comment il est entré dans le réseau et ce qu'il peut faire pour combler les failles.

Comment la cybersécurité peut-elle prévenir ou se défendre contre les attaques de piratage informatique Black Hat ?

Les hackers Black Hat représentent une menace importante pour les organisations.

Cependant, il existe des mesures de cybersécurité qui aident à empêcher les tentatives de piratage Black Hat d'accéder aux réseaux ou de dépasser le point de violation initial, telles que :

- **Pare-feux nouvelle génération (NGFW)**
- **Filtres de contenu**
- **Systèmes de prévention des intrusions (IPS)**
- **Renforcement du serveur**
- **Politiques d'utilisation des ordinateurs**
- **Tests de sécurité**
- **Formation de sensibilisation des employés**
- **Micro-segmentation:** diviser un réseau en segments isolés, au niveau des **applications**, des **charges de travail**, ou des **hôtes individuels**
- **Un accès ZTNA (Zero-Trust network access):** modèle de sécurité qui repose sur le principe de **"ne jamais faire confiance, toujours vérifier"**. Contrairement aux réseaux traditionnels, où les utilisateurs internes sont considérés comme fiables une fois authentifiés
- **Sécurité des endpoints:** Ensemble des stratégies, solutions et pratiques mises en place pour protéger les **appareils connectés** à un réseau (ordinateurs, smartphones, tablettes, objets connectés, etc.)

2- Hackers white hat :

Les **hackers white hat** (ou **hackers éthiques**) sont des **experts en cybersécurité** qui utilisent leurs compétences en piratage pour:

- **protéger les systèmes**,
- **identifier les vulnérabilités**,
- **aider les organisations** à améliorer leur sécurité.

Contrairement aux **black hats** (pirates malveillants), les **white hats** agissent avec **l'autorisation** des propriétaires des systèmes.

Caractéristiques des hackers white hat :

1- Objectifs légaux :
Leur **activité est approuvée** des **lois**.

2- Détection des vulnérabilités :
Ils effectuent des **tests d'intrusion** (**pentests**) pour **trouver les failles** avant qu'elles **ne soient exploitées par des hackers malveillants**.

3- Éthique : Leur mission est de **protéger**, non de nuire.

4- Collaboration :
Ils travaillent avec les entreprises, les **gouvernements ou d'autres organisations**.

Activités typiques des hackers white hat :

• Réaliser des audits de sécurité.

• Tester les défenses des réseaux, applications et systèmes (via des pentests).

• Proposer des solutions pour corriger les vulnérabilités.

• Participer à des programmes de **bug bounty**, où ils sont récompensés pour avoir signalé des failles.

Un hacker white hat peut être **engagé** pour **simuler une attaque** et **vérifier si une organisation est capable** de **détecter et bloquer l'intrusion**.

Hackers au chapeau gris :

Ils travaillent à la fois de manière offensive et défensive.

Les **hackers au chapeau gris** (**grey hat hackers**) sont des individus situés entre les **white hats** (hackers éthiques) et les **black hats** (hackers malveillants).

Ils explorent et piratent des systèmes **sans autorisation préalable**, mais **sans intention malveillante**.

Leur objectif est souvent de **signaler les vulnérabilités découvertes**, bien que leurs actions soient techniquement **illégales**.

Caractéristiques des hackers au chapeau gris :

1- Non autorisé :
Ils accèdent à des systèmes ou réseaux sans permission, mais sans intention de nuire.

2- Ethique ambivalente :
Leur motivation est souvent d'aider en signalant les failles, mais leurs méthodes enfreignent les lois.

3- Pas de profit malveillant :
Contrairement aux black hats, ils ne volent pas de données pour un gain personnel ou pour nuire.

Exemple d'activité d'un grey hat :
Un hacker grey hat découvre une faille sur un site web gouvernemental :
Il accède au système sans autorisation pour prouver la vulnérabilité.

Ensuite, il informe l'administration concernée pour corriger le problème.

Cependant, son intrusion reste illégale, même si l'intention est positive.

En bref, les **grey hat hackers** sont des hackers qui **agissent entre le bien et le mal** :
ils découvrent des failles de manière non autorisée, mais souvent pour avertir ou améliorer la sécurité des systèmes.

Script kiddies

Les **script kiddies** sont des **individus** qui pratiquent le piratage informatique sans avoir de compétences techniques avancées.

Ils utilisent des **outils préconçus** ou des scripts créés par d'autres hackers pour effectuer des attaques, souvent sans en comprendre pleinement le fonctionnement.

Caractéristiques des script kiddies :

1. **Manque de compétences** : Ils ne développent pas leurs propres outils ou exploits.

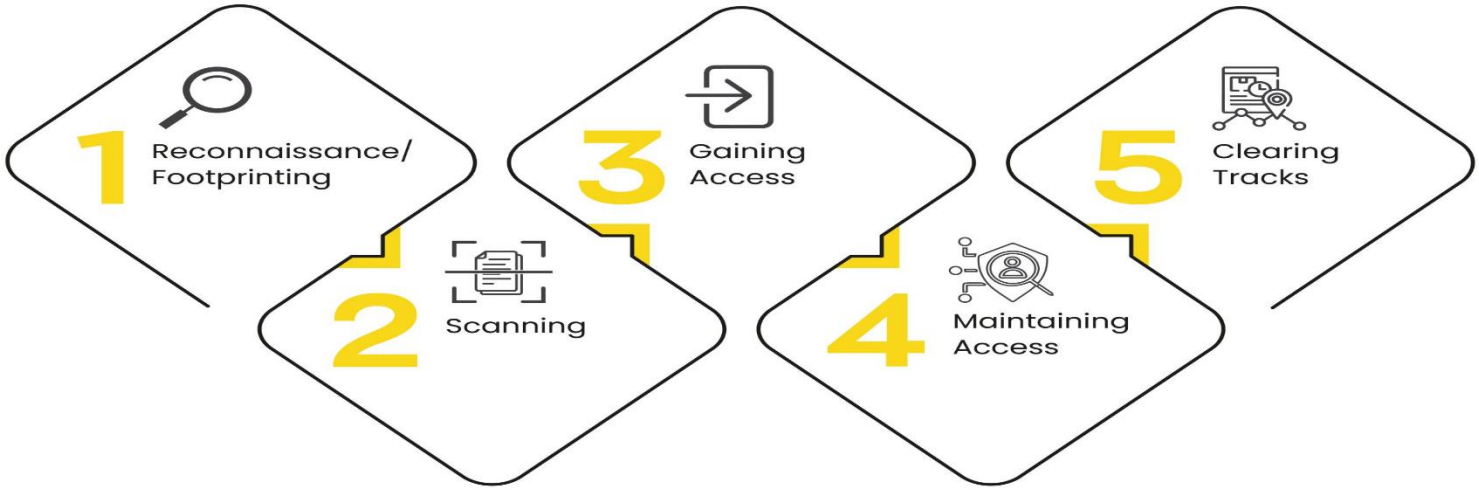
2. **Utilisation d'outils publics** : Ils se servent de logiciels ou scripts accessibles, comme des scanners de vulnérabilités, des outils DDoS (Low Orbit Ion Cannon), ou des kits d'exploits.

3. **Motivations peu sophistiquées** : Ils cherchent souvent à impressionner ou causer des dégâts, plutôt que de poursuivre des objectifs complexes (comme les black hats ou grey hats).

4. **Cibles faciles** : Ils attaquent généralement des systèmes peu sécurisés ou des cibles non critiques

Les phases du piratage (Hacking phases)

Le piratage informatique se déroule principalement en cinq phases .



Il n'est pas forcément nécessaire qu'un pirate informatique suive ces cinq étapes de manière séquentielle.
Il s'agit d'un processus par étapes qui, s'il est suivi, donne de meilleurs résultats.

1. Reconnaissance :

On l'appelle aussi **phase d'identification** et de **collecte d'informations**.

Il s'agit de la **phase préparatoire** au cours de laquelle nous **collectons autant d'informations que possible** sur **la cible**.

Nous collectons généralement des informations sur trois groupes,

- **Réseau**
- **Hôte**
- **Personnes impliquées**

L'attaquant collecte, à partir de nombreuses sources, toutes les **informations sensibles accessibles au public**, telles que :

- **Les clients ciblés**
- **Les employés**
- **Les informations sur le réseau**

À la fin de cette phase, le pirate aura une vue claire du :

- **Réseau** : nom de domaine, plages d'adresses IP, services TCP/UDP, et mécanismes d'authentification.
- **Système** : noms d'utilisateur/groupe, bannières système et architecture système.
- **Informations organisationnelles** : détails des employés, communiqués de presse et localisation.

Pour la phase reconnaissance, existe **deux types d'empreintes** :

Reconnaissance Actif :
interagir directement avec la cible pour recueillir des informations sur la cible.
Par exemple,
utiliser **l'outil Nmap** pour analyser la cible

Reconnaissance Passif :
Tenter de collecter des informations sur la cible sans y accéder directement.
Cela implique de collecter des informations à partir des réseaux sociaux, des sites Web publics, etc.

La reconnaissance peut inclure **des méthodes** comme **contacter** le **support technique** pour obtenir des **informations sensibles**.

Cependant, la reconnaissance n'est pas seulement technique.
C'est également une arme importante de **renseignement concurrentiel**.
Connaître certains aspects **financiers** de la cible peut significativement augmenter les chances de réussite de l'attaque.

2- Scanning (Analyse des failles)

Le **scanning** est une **phase clé** du processus de **piratage** (ou de **test d'intrusion**) où un **attaquant ou un testeur de sécurité** effectue une **analyse approfondie d'un système, d'un réseau ou d'une application** pour identifier des **vulnérabilités exploitables**.

Objectif du scanning :

- **Identifier les ports ouverts** :

Déterminer quels services (HTTP, FTP, SSH, etc.) sont actifs sur une machine cible.

- **Découvrir les vulnérabilités** :

Trouver des failles dans les services, applications ou systèmes d'exploitation.

- **Obtenir des détails précis** :

Versions des logiciels, systèmes d'exploitation, configurations incorrectes.

Types de scanning :

Scanning des ports, Scanning réseau, Scanning des vulnérabilités et **Scanning d'applications Web**

a- Scanning des ports :

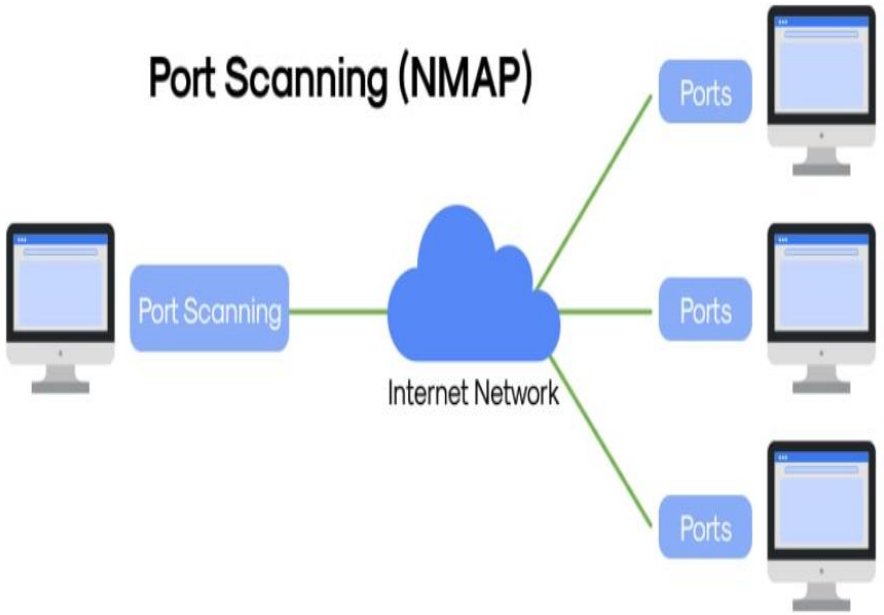
L'analyse des ports est le processus d'**envoi de paquets à une cible** dans le but d'en **savoir** plus sur celle-ci en **association** avec des **numéros de port bien connus**.

Il existe deux catégories d'analyse de ports :
Analyse TCP et **Analyse UDP**

- Vérifie quels **ports réseau** (ex. : **80 pour HTTP, 22 pour SSH**) sont **ouverts**.

- Utilise des outils comme **Nmap**, **Netcat** ou **Zenmap**.

Exemple : Un port SSH ouvert peut indiquer une cible potentielle pour une attaque brute-force.



b- Scanning réseau :

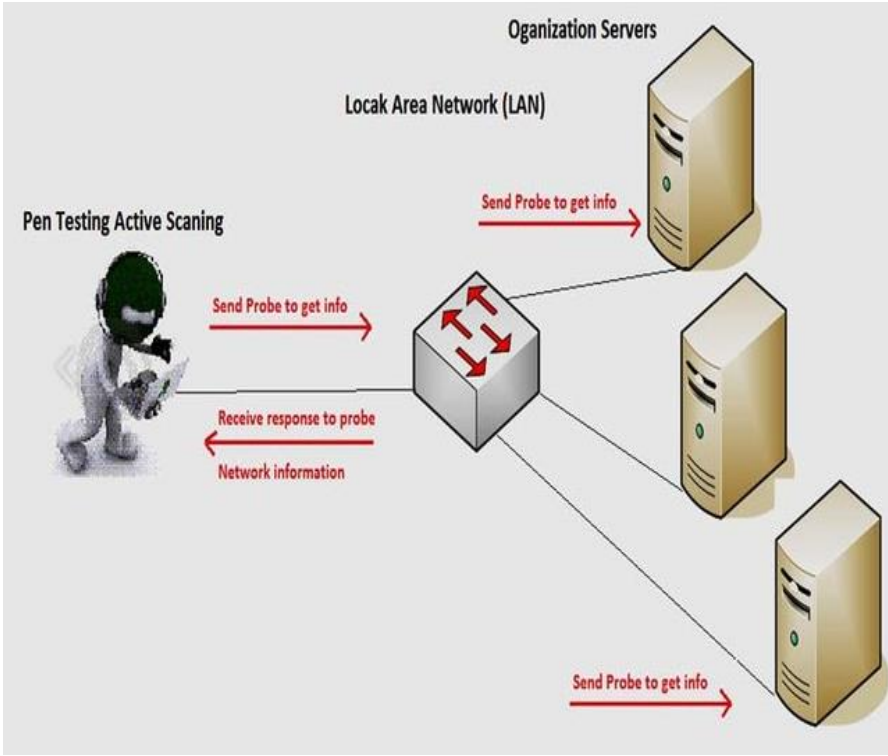
L'analyse réseau c'est le processus de **localisation de tous les hôtes actifs sur un réseau**.
Un type courant d'analyse réseau est l'**analyse d'une plage d'adresses IP**.

- **La technique** de base pour **découvrir les hôtes actifs** est le **balayage ping**, qui consiste à **envoyer** des **requêtes d'écho ICMP** à **plusieurs hôtes** à partir d'une **plage d'adresses IP**.

Exemple: Outils **Hping2** est un scanner réseau en ligne de commande simple, conçu pour le protocole **TCP/IP**.

- Cartographie les **adresses IP**, les sous-réseaux et les dispositifs actifs.

- Permet de détecter l'architecture du réseau cible (topologie).



c- Scanning des vulnérabilités :

Le **scanning des vulnérabilités** est le processus d'**analyse d'un système, réseau, application ou appareil** pour identifier des **failles de sécurité potentielles**.

Ces failles, appelées **vulnérabilités**, pourraient être **exploitées par des attaquants** pour accéder au système, le compromettre ou en voler les données.

- Recherche des services obsolètes ou des configurations vulnérables.

- Utilise des outils comme
Nessus,
OpenVAS,
Qualys
...

Objectifs du scanning des vulnérabilités :

1.Identifier les faiblesses :
Détecter les logiciels obsolètes, les mauvaises configurations ou les services vulnérables.

1.Évaluer le risque :
Déterminer la gravité des vulnérabilités identifiées (critique, élevée, moyenne, faible).

1.Prioriser les corrections :
Aider les équipes à corriger en priorité les failles les plus critiques.

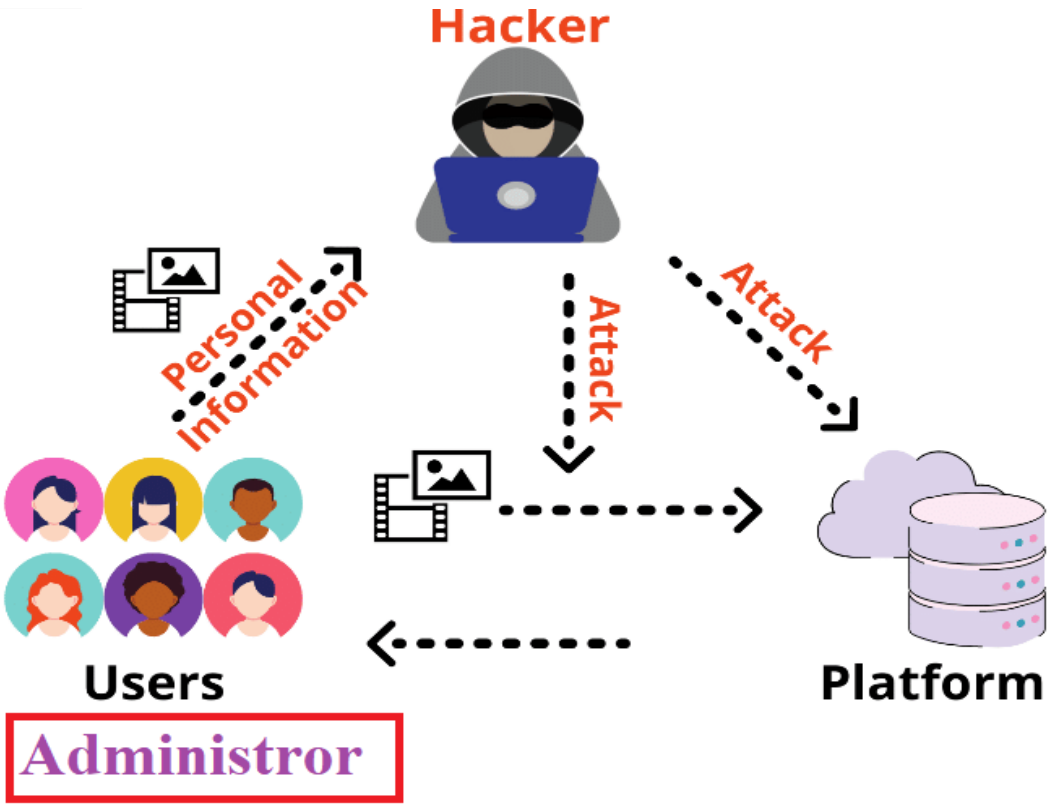
1.Prévenir les attaques :
Réduire la surface d'attaque avant qu'un pirate ne puisse exploiter les failles.

3. Gaining Access (Obtenir l'accès)

C'est la phase où un **attaquant** tente d'obtenir un **accès non autorisé à un système**, un **réseau** ou **une application** après avoir **collecté des informations sur la cible**.

Dans cette phase, **l'attaquant s'introduit** dans **le système/réseau** à l'aide de **divers outils ou méthodes**.

Après être entré dans un système, il doit **augmenter ses privilèges** au **niveau administrateur** afin de **pouvoir installer une application.**



4. Maintien de l'accès (Maintaining Access) :

C'est mettre en place des **mécanismes** pour **garder un accès persistant** à la **cible** en arrière-plan. Cela lui **permet de revenir ultérieurement**, même si la faille initiale est corrigée ou si les systèmes sont redémarrés.

Techniques courantes pour maintenir l'accès :

1- Installation de backdoors :

- Les backdoors (portes dérobées) permettent un accès secret au système via des ports spécifiques ou des commandes.

Exemple : Création d'un compte administrateur caché ou installation d'un logiciel malveillant.

2- Utilisation de malwares :

- Déploiement de malwares comme des trojans, rootkits, ou ransomwares.
- Ces programmes **s'exécutent en arrière-plan** pour **offrir un accès continu** à **l'attaquant**.

3- Tunnels chiffrés :

Mise en place de connexions VPN ou de tunnels SSH pour rester connecté discrètement.

4- Escalade de privilèges :

Obtenir des droits d'administrateur pour créer des mécanismes d'accès permanents.

5- Modification des configurations système :

Altérer les fichiers système ou les paramètres de sécurité pour désactiver les alertes et éviter la détection.

6- Persistance sur le réseau :

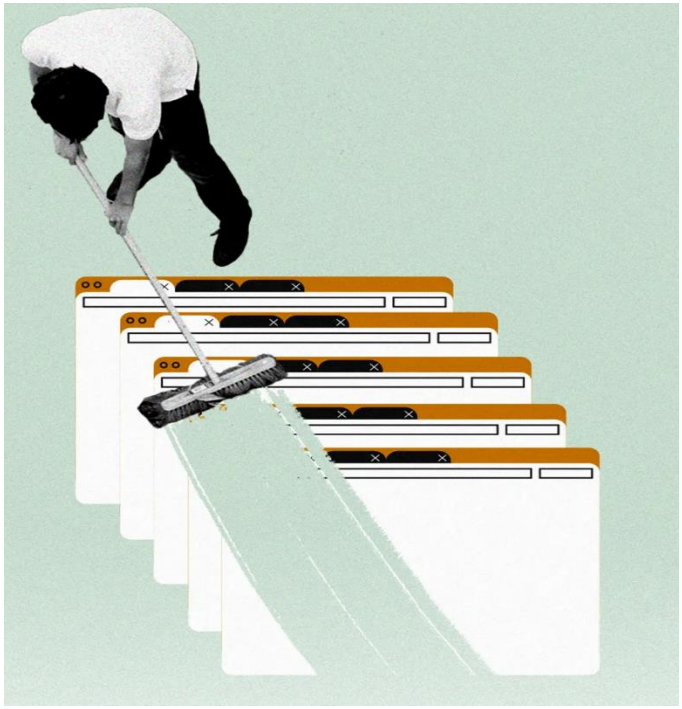
Infection de plusieurs machines pour garantir un accès même si un appareil compromis est corrigé.

Clearing tracks (Dégagement de la piste)

Un pirate informatique intelligent <u>efface</u> toujours toutes les **preuves** que **personne ne trouve de traces** menant à lui.

Principe: Le pirate se concentre sur la **modification/corruption/suppression:**

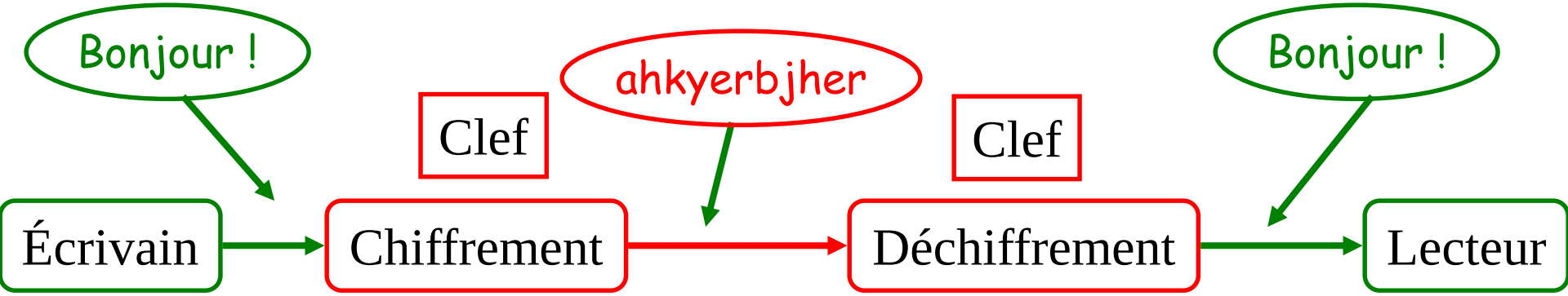
- des valeurs des journaux,
- la modification des valeurs du registre,
- la désinstallation de toutes les applications utilisées et
- la suppression de tous les dossiers créés.
- Désactive les mécanismes d'audit.
- …



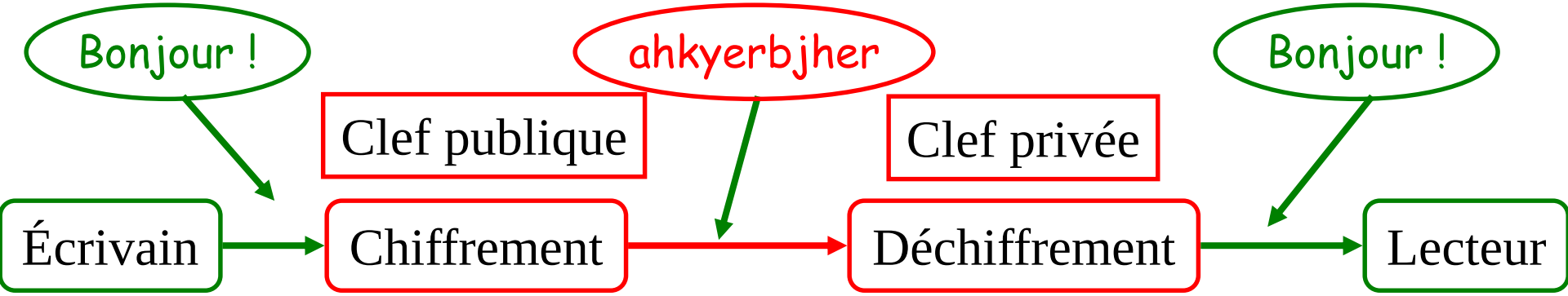
Chiffrement et clés

Principe du chiffrement

- Chiffrement symétrique : on utilise la même clés pour chiffrer et pour déchiffrer



- Chiffrement asymétrique : on chiffre avec la clés publique et on déchiffre avec la clés privée



Histoire du chiffrement

- Le chiffrement de César (décalage de lettres)
- Disque de chiffrement (Léone Battista Alberti en 1466)

- 1940, le chiffrement par machine, exemple Enigma. Début de la cryptanalyse.

Protocole à clés publique

- **Protocole d'authentification** (prouvé l'un et l'autre leurs identités respectives dans un réseau non sûr) inventé par Needham-Schroeder en 1978

- Il a fallu 17 ans pour l'imaginer et ce rendre compte que l'étude des **protocoles cryptographiques** est un vrai challenge (pas un protocole au monde n'est à 100% sûr…)

Chiffrement aujourd'hui

Utilisation de problème algorithmique dure (en temps de calcul). Essentiellement basé sur les nombres premiers (divisible que par 1 et par eux-même)

Chiffrement à clé publique

Protocole

- **Algorithme de génération des clés** $\mathcal{KG}(\ell) = (\mathsf{pk}, \mathsf{sk})$

à partir d'un paramètre de sécurité, il produit une paire de clés

- **Algorithme de chiffrement** $\mathcal{E}(\mathsf{pk}, m) = c$

produit le chiffré d'un message m, par la clé publique

- **Algorithme de déchiffrement** $\mathcal{D}(\mathsf{sk}, c) = m$

utilise la clé sécrete/privée sk pour retrouver m à partir de c

Chiffrement aujourd'hui

Exemple: Protocole RSA

RSA - Génération des clés

$\mathcal{KG}(\ell) = (\mathsf{pk}, \mathsf{sk})$

- Soit $n = p \cdot q$ (p et q premiers)
- L'ordre du groupe multiplicatif $\mathbb{Z}_n^\star = \varphi(n) = (p-1)(q-1)$
- Soit e un entier premier avec $\varphi(n) = (p-1)(q-1)$
- Soit d un entier qui satisfait $d \cdot e = 1 \pmod{\varphi(n)}$

$$d \cdot e + u\varphi(n) = 1 \qquad \text{(Bézout)}$$

clé publique

- $n = pq$: module public
- e : exposant public

clé secrète

- $d = e^{-1} \pmod{\varphi(n)}$
- les premiers p et q

Protocole RSA

RSA - Chiffrement

$$\mathcal{E}(\mathsf{pk} = (e, n), M) = M^e \pmod{\mathsf{n}}$$

RSA - Déchiffrement

$$\mathcal{D}(\mathsf{sk} = \mathsf{d}, C) = C^d \pmod{\mathsf{n}}$$

Vérification

$$(M^e)^d = M^{ed} = M^{1-u\varphi(n)} = M \cdot 1 = M \pmod{n}$$

(Théorème d'Euler)

Conséquences

- Casser ce type de cryptage est très très très très très long, exponentiel en la taille de la clés

- Environ 2^60 ans pour une clés de 1024 bits soit environ 11529215046 milliards d’années

Sécurité et Sûreté

Sécurité Informatique

Prévenir et empecher les risques et conséquences :

- d'un événement accidentel ou involontaire tel que la destruction
- la dégradation du système d'information suite à un incendie, une inondation, la panne d'un équipement
- la suppression involontaire de documents informatiques.

La politique de sécurité informatique repose sur des outils et s'appuie sur l'information dispensée aux collaborateurs.

Sûreté et sécurité

Sûreté Informatique

Définie la **prévention des actes volontaires** par l'association:

- **de moyens humaines,**
- **de solutions techniques et organisationnelles**

Contre Les risques de :

- vol de donnée informatique,
- Le piratage et l'intrusion dans un système informatique
- le blocage des moyens de communication de l'entreprise.

Futur pour la sécurité?

Informatique quantique

L'informatique quantique est considérée comme une **menace importante**.

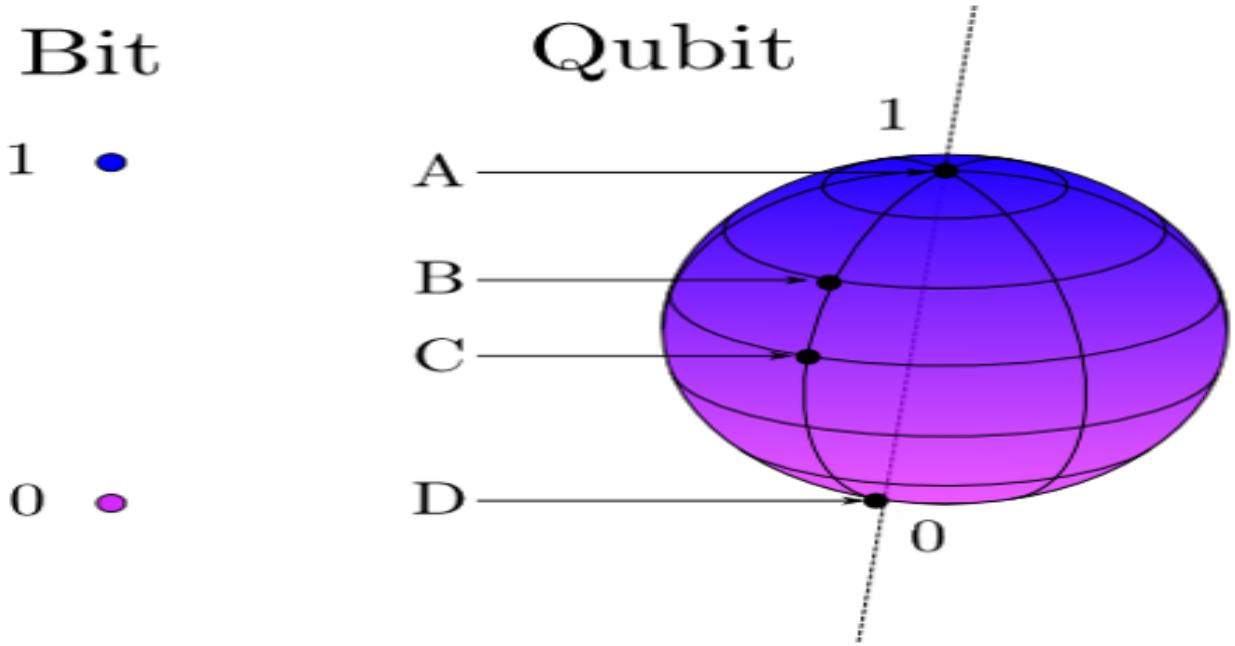
L'ordinateur quantique pourrait facilement casser les plus sophistiqués de nos codes secrets.

Un code généré à travers cette technologie sera extrêmement fiable

L'informatique quantique comme outil de sécurité

La lutte contre la fraude est aujourd'hui l'une des principales problématiques de sécurité du secteur bancaire.

Aujourd'hui, les ordinateurs quantique constitue un **pilier de la lutte contre la fraude**, à travers leur forte capacité (théorique) de stockage et leur rapidité de traitement.



Un bit peut seulement prendre les valeurs 1 et 0

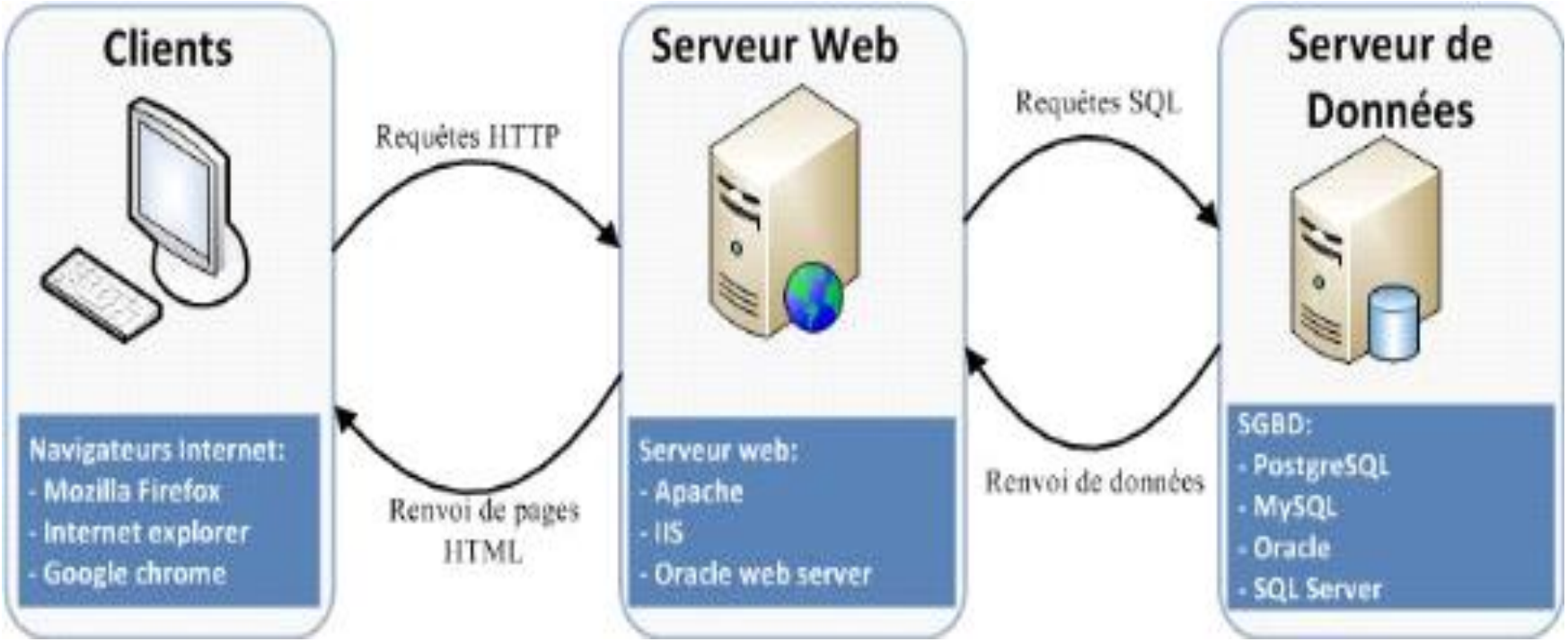
La superposition des états à l'aide de qubits peut être représentée n'importe où sur la sphère

Sécurité des applications Web

SGBD et applications Web

• La très grande majorité des sites Web repose sur du stockage des données dans un SGBD

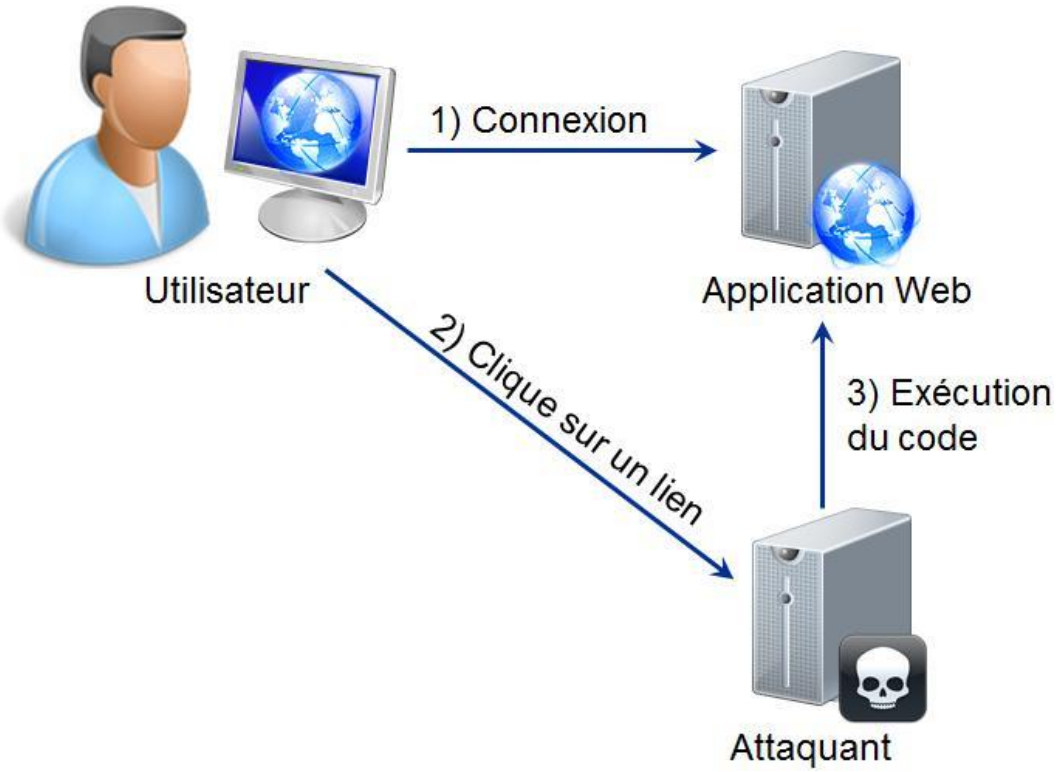
• Réciproquement, la très grande majorité des applications développées au-dessus d'une base de données sont des applications Web



Sécurité côté client

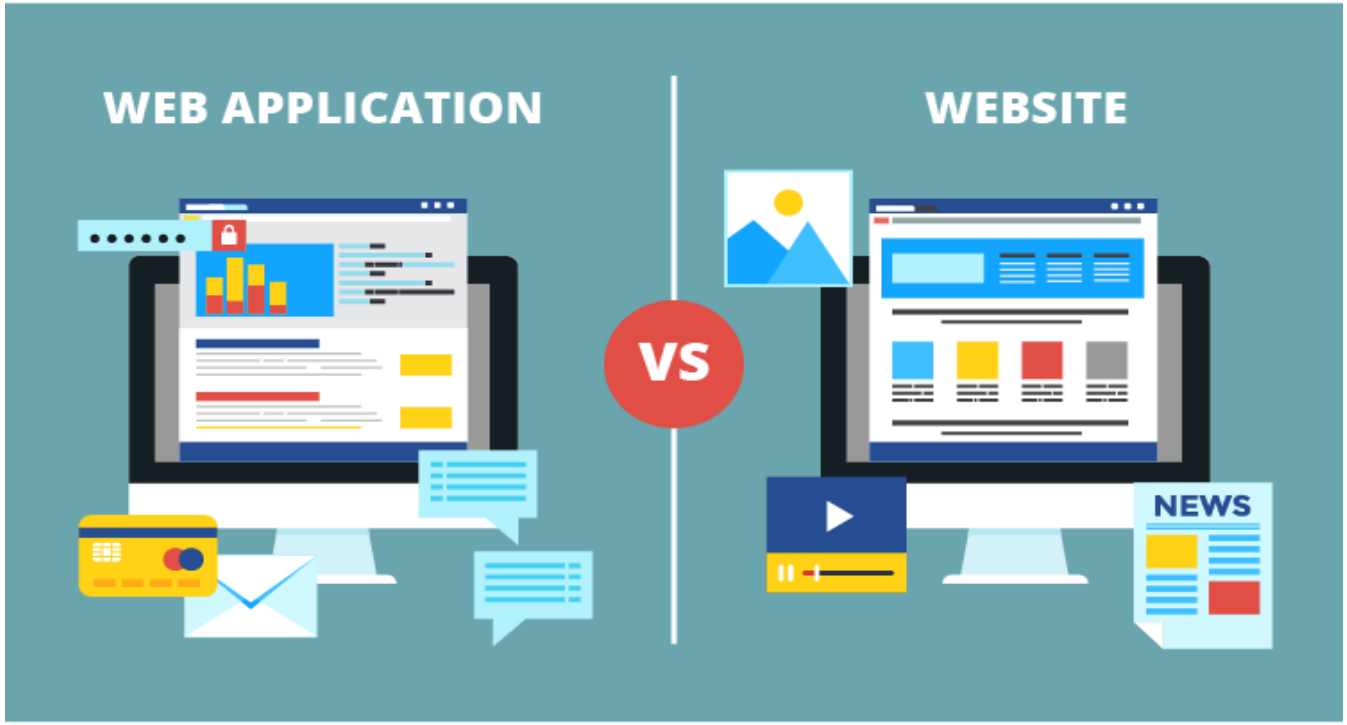
• N’importe qui peut créer un site Web et s’arranger pour qu’il soit référencé par les moteurs de recherche. . . y compris des personnes malveillantes.

• Mais cette protection n’est pas toujours parfaite.



Pas de restriction d'origine pour :

- le chargement d'images, vidéos, et applets
- le chargement de scripts CSS
- les <**iframe**> HTML
- le chargement d'un script JavaScript avec la balise <**script**>
- Les cookies fonctionnent de manière plus libérale
- Les plugins Flash, Silverlight, Java, etc., implémentent une politique d'interaction similaire. . . mais avec des différences de comportement parfois dangereuses



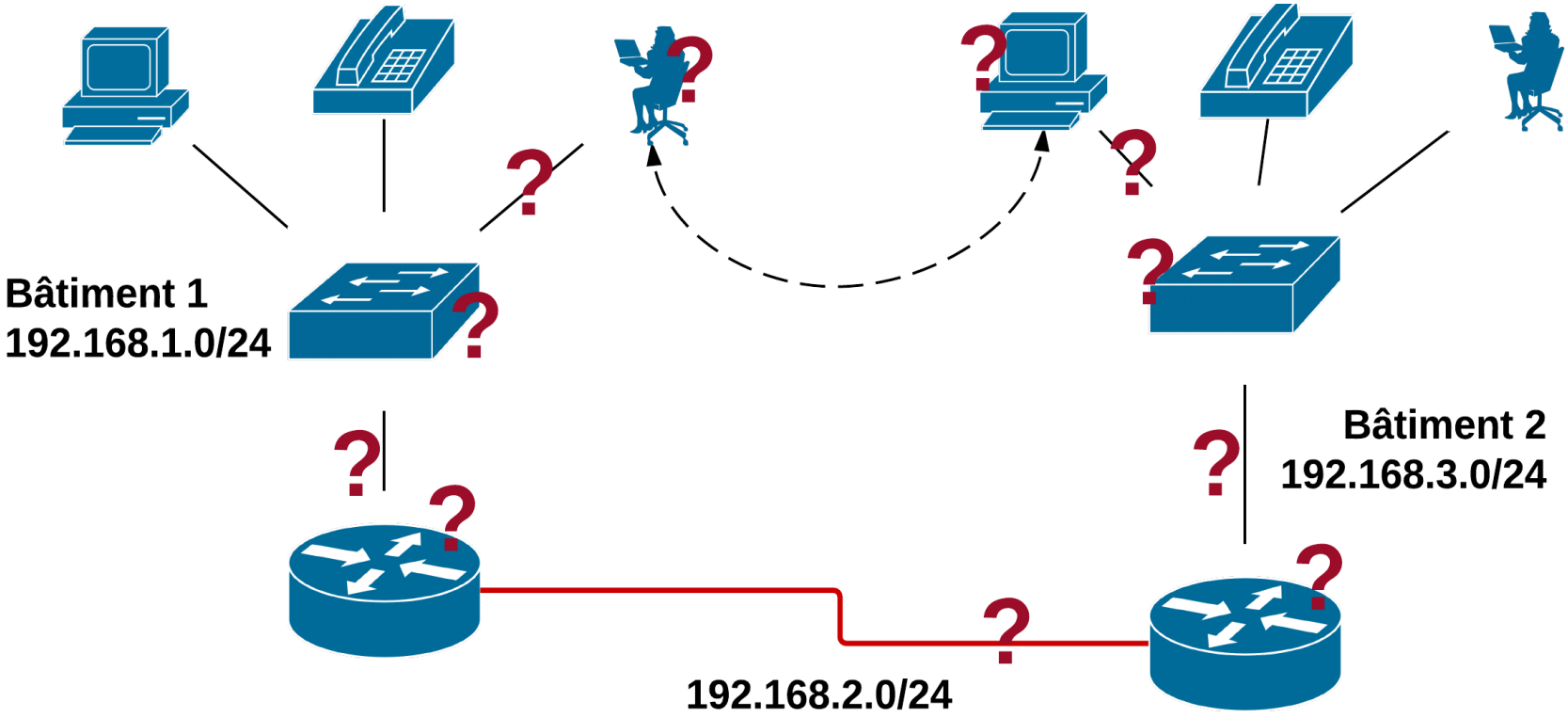
Risques côté client

• Mauvais fonctionnement des logiciels
• Vol dedonnées confidentielles (mots de passe, numéros de carte de crédit, adresses e-mail, etc.)
• Perte de données locales (vandalisme, rançonnement)
• Réutiliser les identifiants d'un utilisateur auprès d'un autre site pour envoyer des mails malicieux, passer des ordres de virement, faire des achats, etc.
• Stockage de données illégales
• Relais pour d'autres formes d'attaques
• …

Capture de paquets IP

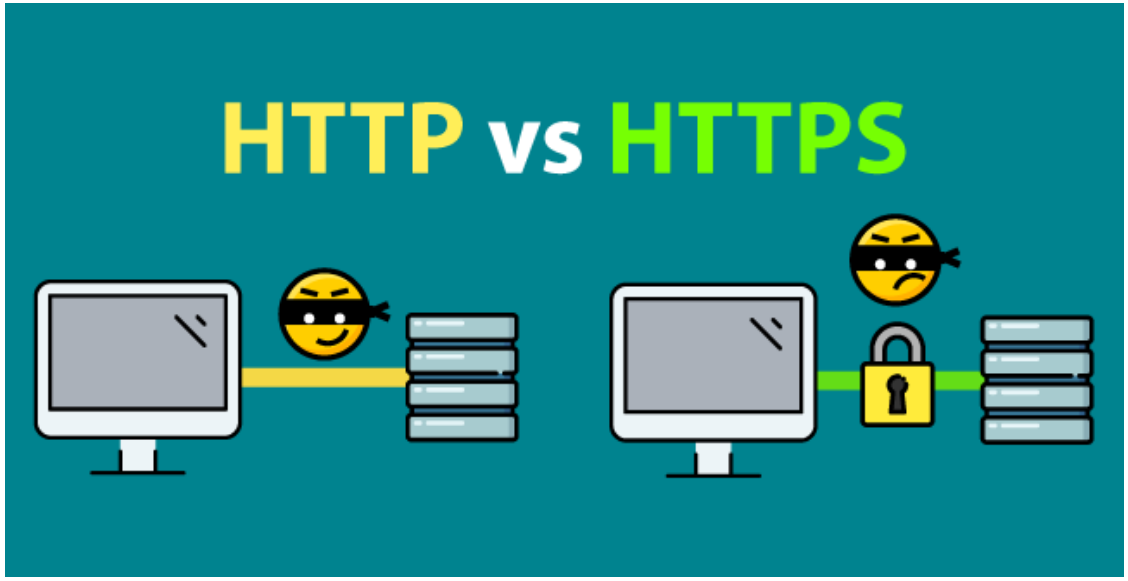
Problème

Sur un réseau local, ou sur un réseau WiFi non chiffré (ou avec un chiffrement WEP simple à casser), il est possible à un attaquant de regarder le contenu des paquets IP en clair, contenant l'ensemble de la communication entre le navigateur et le serveur Web, y compris l'ensemble des paramètres HTTP, etc.



Solution

Ne pas utiliser HTTP pour transmettre des informations sensibles au travers d'Internet, d'autant plus dans le cadre d'un réseau local ou sans fil.



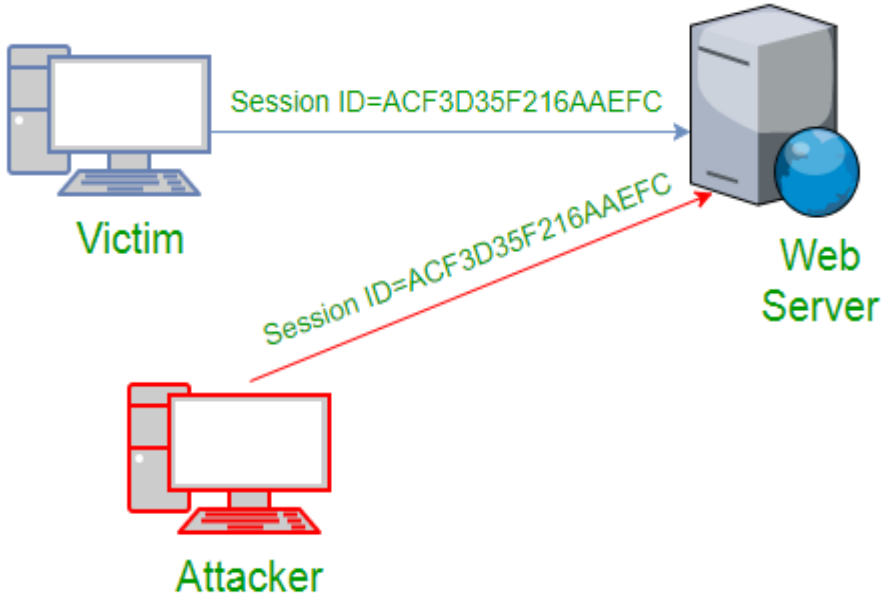
HTTPS, un autre protocole permettant l'envoi chiffré de messages sur le Web

HTTPS permet au visiteur de vérifier l'identité du site web auquel il accède, grâce à un certificat

Usurpation de session

Problème

Différents techniques existent (exemple capture de paquets IP) pour récupérer l'identifiant de session d'un utilisateur (identifiant ordinairement stocké dans un cookie)



Solution

Résoudre les autres problèmes ! Côté serveur, prévoir la possibilité de terminer la session (en PHP, JSP, avec session_destroy) dès que celle-ci n'est plus nécessaire.

Prévention et résolution des pannes

Prévention (1)

- Passer périodiquement un logiciel antivirus récent sur son PC
- Passez cet anti-virus sur les disques (clés USB, CD/DVD etc.) introduit dans votre PC, même ceux de vos proches
- Enregistrer régulièrement son document de travail
- Effectuer des sauvegardes de ses documents sur différents supports (tout support magnétique ou CD/DVD)
- Toujours éteindre son PC par le menu Démarrer/Arrêter ; ne pas l'éteindre avec le bouton On/Off
- Évitez d'avoir trop de documents ou programmes ouverts à la fois ce qui peut surcharger la mémoire

Prévention (2)

- Se méfier des fichiers attachés reçus par courrier électronique (un document Word ou Excel peut contenir des virus macros, un programme exécutable n'importe quel type de virus) ; ne jamais lancer un programme reçu par un expéditeur inconnu
- D'une manière générale, respecter le matériel, ne pas lui demander de faire trop de choses à la fois
- Désinstallez proprement vos logiciels (Ajout/Suppression de programmes dans le panneau de configuration)

Résolution (1)

- **Dysfonctionnement d'un logiciel** : enregistrer son travail, quitter le logiciel et le relancer

- **Blocage** : si la souris fonctionne, essayer de quitter le logiciel ; pressez Alt-Tab pour changer d'application si vous avez un document à sauver; si rien ne marche appuyer sur les touches Control-Alt-Suppr (1 seconde au moins). La liste des programmes actifs s'affiche alors. Sélectionnez celui indiquant *(pas de réponse)* et cliquez sur *fin de tâche*. Les travaux en cours sur ce logiciel risquent d'être perdus.

- Si Control-Alt-Suppr ne marche pas, il ne reste plus qu'à arrêter l'ordinateur (bouton On/Off ou mieux : bouton Reset) ;

Résolution (3)

- Si vous avez un virus : désinfectez tous les supports infectés (disque dur, disquettes) et affichez le descriptif du virus (il peut être bénin ou très dangereux) ;

- Si Windows ne démarre pas : démarrez en mode « sans échec » (touche F8 ou Control sous Windows) ; si le PC démarre il s'agit d'un problème de pilote de périphérique ; utiliser l'aide de Windows et les programmes utilitaires