Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Bejaia
Faculté des Sciences Exactes
Département d'Informatique

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Sécurité des systèmes d'information

Enseignante: **Dr N. YESSAD**

Niveau: Master 2 option SIA

Année universitaire: 2022-2023

Objectifs du module

- Maîtriser les notions de base relatives **à la sécurité**
- Connaître **les objectifs** de la sécurité et **les mécanismes** à mettre en place pour assurer la sécurité des systèmes d'information
- Présenter les **aspects techniques**, organisationnels, méthodologiques à la sécurisation des systèmes d'information et des réseaux.
- Bien comprendre les **attaques /intrusions** et leurs **conséquences** sur les systèmes d'information.

Contenu du module

Chapitre 1: Introduction à la sécurité dans un système d'Information

Chapitre 2: Quelques méthodes de protection de l'information

Chapitre 3: Identification des vulnérabilités d'un système d'information

Chapitre 4: Politique de sécurité

Chapitre 5: Détection, évaluation et notification des intrusions

Chapitre 6: Sécurité d'un point de vue juridique

Chapitre 1

Introduction à la sécurité des systèmes d'information

Contenu du chapitre

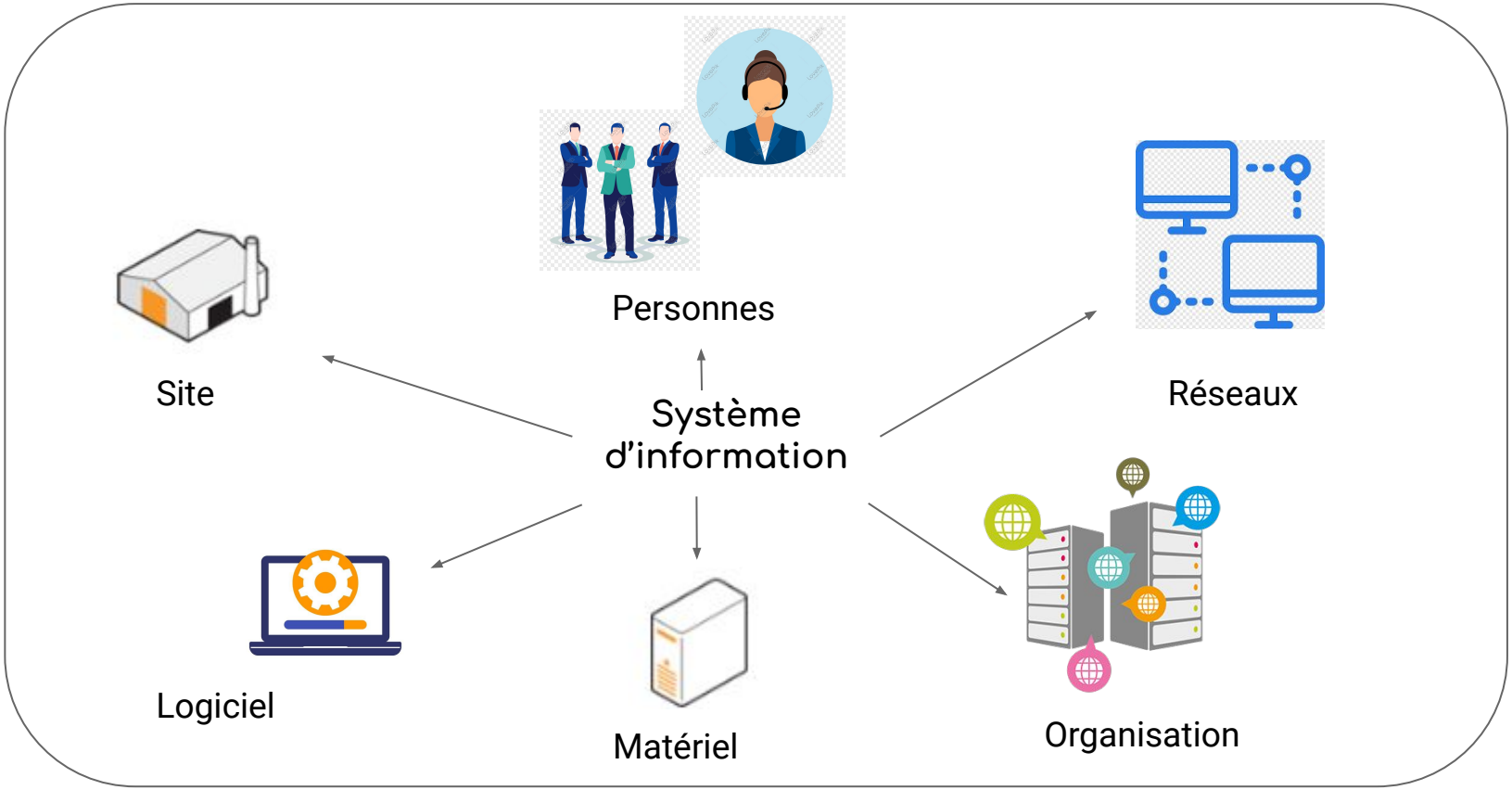
- ★ Introduction
- ★ Système d'information
- ★ Sécurité d'un système d'information (SSI)
- ★ Services et objectifs de SSI
- ★ Enjeux de SSI
- ★ Concepts de SSI
- ★ Menaces
- ★ Attaques
- ★ Conclusion

Introduction

La Sécurité des systèmes d'information est un domaine extrêmement vaste puisqu'elle fait appel à de **nombreux concepts** juridiques, sociaux, et économiques, à la gestion de personnel, et à des connaissances techniques extrêmement pointues.

Système d'information

➔ Un système d'information **(noté SI)** représente l'ensemble organisé de ressources (**personnel, données, procédures, matériels, logiciels, réseaux, applications, bases de données etc.**) destinées à collecter, classifier, stocker, gérer, diffuser **les informations** au sein d'une organisation


Personnes
Site
Réseaux
Système d'information
Logiciel
Matériel
Organisation

Le périmètre du terme SI peut être très différent d'une organisation à une autre et peut recouvrir selon les cas tout ou partie des éléments suivants:

- Bases de données de l'organisation,
- Applications métiers,
- Infrastructure réseau,
- Serveurs de données
- Systèmes de stockage,
- Serveurs d'application,
- Dispositifs de sécurité, etc

La sécurité du SI consiste donc à assurer la sécurité de l'ensemble de ces biens

Les causes de fragilité des SI

- Mauvais fonctionnement du matériel informatique (Une panne du matériel informatique, etc);
- Mauvais fonctionnement des logiciels (une installation mal faite, etc);
- Désastres (Des pannes de courant, inondations, incendies et autres catastrophes naturelles);
- Impartition (Faire appel à des sous-traitants locaux ou à l' ´etranger), etc.

Pourquoi les SI sont-ils atteints ?

Les motivations évoluent !!!! De nos jours majoritairement des actions organisées et réfléchies pour des finalité de:

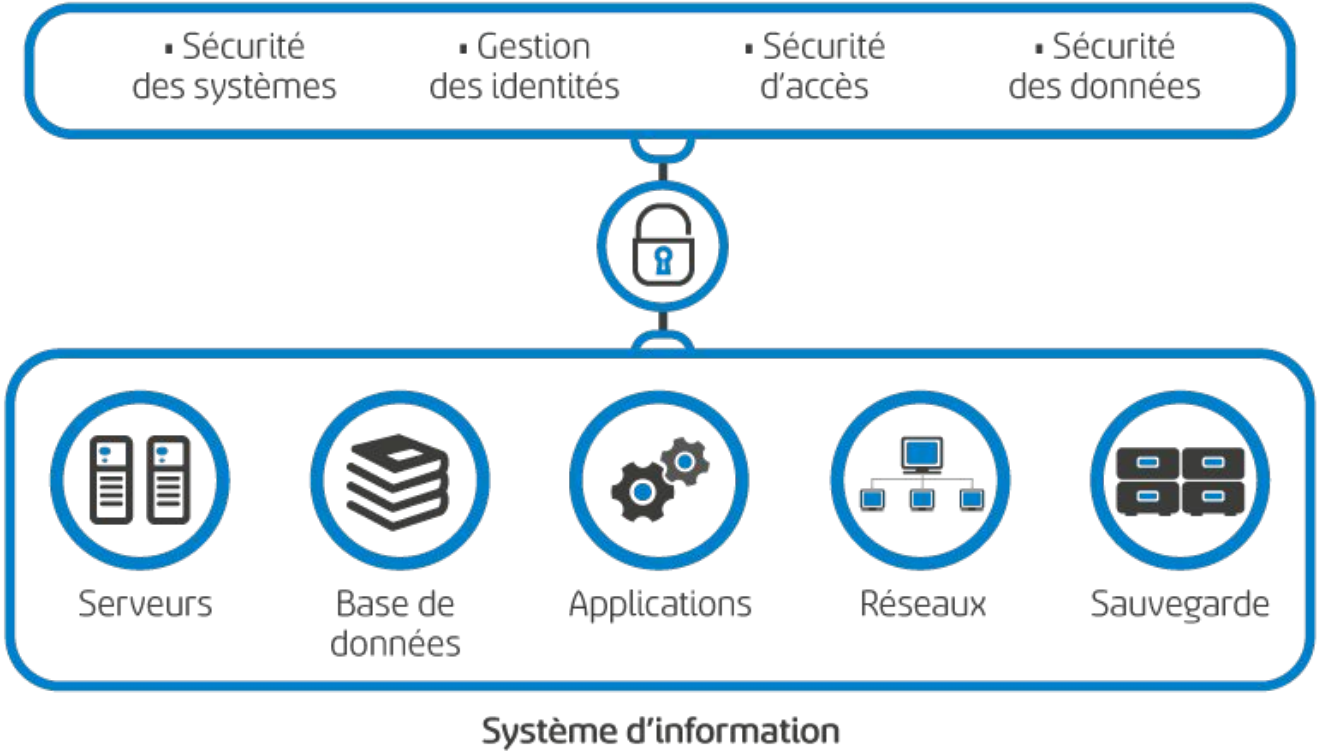
Gains financier	utilisation des ressources	Chantage	Espionnage
accès à l'information, puis **monétisation et revente**) l'utilisation des emails fichiers clients, comptes bancaire, divulgation de l'organisation interne;	l'utilisation de Bande passante et espace de stockage (hébergement de musique, films et autres contenus)	(Déni de service, Modifications des données);	Industriel / concurrentiel, Étatique),etc.

Sécurité des Systèmes d'information

- Sécurité des systèmes d'information **noté (SSI)**

- Ensemble de méthodes, **techniques ,organisationnels, juridiques et humains** nécessaires et mis en place pour conserver, rétablir, garantir et **protéger** les ressources d'un système d'information.

- Moyens visant à empêcher l'utilisation **non autorisée, le mauvais usage, la modification ou le détournement du système d'information.**



Sécurité des Systèmes d'information

SSI est-elle une affaire d' informaticiens ?

- ➔ SSI **n'est plus confinée** uniquement au rôle de l'informaticien. Elle **implique tout le monde**, à différents degrés.

- ➔ Le personnel doit donc **être sensibilisé aux enjeux de la SSI** car ils définissent la nature de la protection à adopter face aux différents risques.
- ➔ Sa finalité sur:
  - ❖ Le long terme est de maintenir la confiance des utilisateurs et des clients.
  - ❖ Le moyen terme est la cohérence de l'ensemble du système d'information.
  - ❖ Le court terme, l'objectif est que chacun ait accès aux informations dont il a besoin.

Services & Objectifs de SSI

- **Authenticité**

l'authentification qui assure **que seules les personnes habilitées aient accès aux ressources** (les utilisateurs doivent prouver leur identité par l'usage de code d'accès). Cela permet de gérer les droits d'accès aux ressources concernées et maintenir la confiance dans les relations d'échange.

- **Confidentialité**

➔ les informations n'appartiennent pas à tout le monde
➔ Seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées.
➔ Tout accès indésirable doit être empêché.

- **Intégrité**

l'intégrité du système et de l'information traitée qui garantit que ceux-ci **ne sont modifiés que par une action volontaire et légitime,**

- **Non répudiation**

la non-répudiation qui garantit qu'aucun des acteurs **ne pourra nier** avoir effectué une action sur le système,

- **Disponibilité**

la propriété d'un système ou une ressource système accessible et utilisable à la demande par une entité système autorisée.

- **Traçabilité (ou " Preuve ")**

garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

Lorsque l'on fait de la SSI, on se pose principalement deux questions :

Qu'est-ce que je veux protéger ?

Pourquoi je veux où je dois le protéger ?

En **répondant** à ces questions les directions métiers expriment des besoins de sécurité qui sont déclinés en objectifs et **mesures de sécurité**, la sécurité s'aligne ainsi sur la stratégie de l' établissement.

Degré de sécurité

Comment peut-on évaluer le degré de sécurité d'une ressource d'un SI ?

il faut **auditer son niveau** de **Disponibilité**, **Intégrité**, **Confidentialité** , **non répudiation** et de **Preuve**. L'évaluation de ces critères sur une échelle permet de déterminer si ce bien est **correctement sécurisé**.

Exemple :
Résultats d'un audit sur un bien sur une échelle (Faible, Moyen, Fort, Très fort):
Niveau de Disponibilité du bien: Très fort
Niveau d'Intégrité du bien: Moyen
Niveau de Confidentialité du bien: Très fort
Niveau de Preuve du bien: Faible

Le bien bénéficie d'un niveau de sécurité adéquat

Exemple:

Pour un Un site institutionnel simple statique d'une organisation qui souhaite promouvoir ses services sur internet

Disponibilité

"très fort" : un haut niveau de disponibilité du site web est nécessaire, sans quoi l'entreprise ne peut atteindre son objectif de faire connaître ses services au public

Confidentialité

"Faible" un faible niveau de confidentialité suffit. en effet les informations contenues dans ce site sont publiques par nature !

Intégrité

"Très fort" un haut niveau d'intégrité des informations présentées est nécessaire. en effet , l'entreprise ne souhaitait pas qu'un concurrent modifier frauduleusement le contenu du site web pour y insérer des informations erronées

Preuve

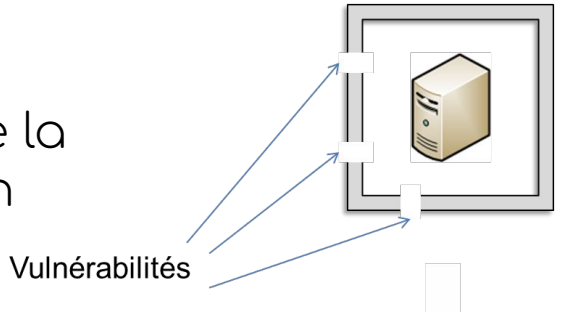
"Faible" niveau de preuve suffit en effet de site web ne permet aucune interaction avec les utilisateurs il fournit simplement des informations fixes

Degré de sécurité

Concepts de la SSI

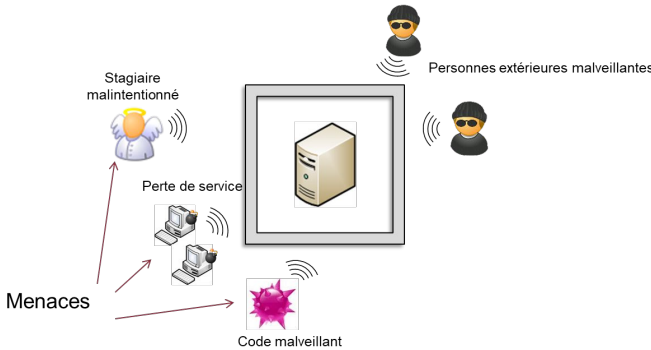
Vulnérabilité

Faiblesse ou faille au niveau d'un bien (conception, réalisation, installation, de la configuration ou de l'utilisation du bien



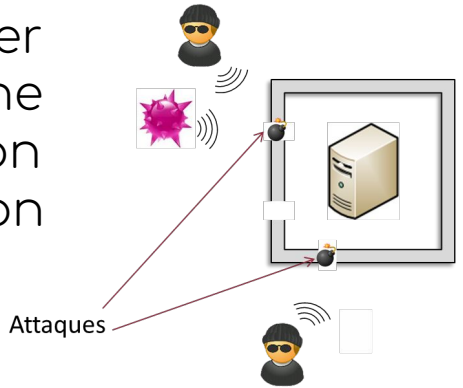
Menace

Peut être définie comme une cause potentielle d'un incident, qui pourrait entraîner des dommages sur un bien si cette menace se concrétise



Attaque

Action malveillante destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la concrétisation d'une menace, et nécessite l'exploitation d'une vulnérabilité.



Risque

Le risque c'est l'opportunité de l'exploitation par une menace d'une vulnérabilité qui affecte un bien.

Contre mesures

C'est l'ensemble de moyens mis en place pour faire face aux risques dans une organisation.

Incident

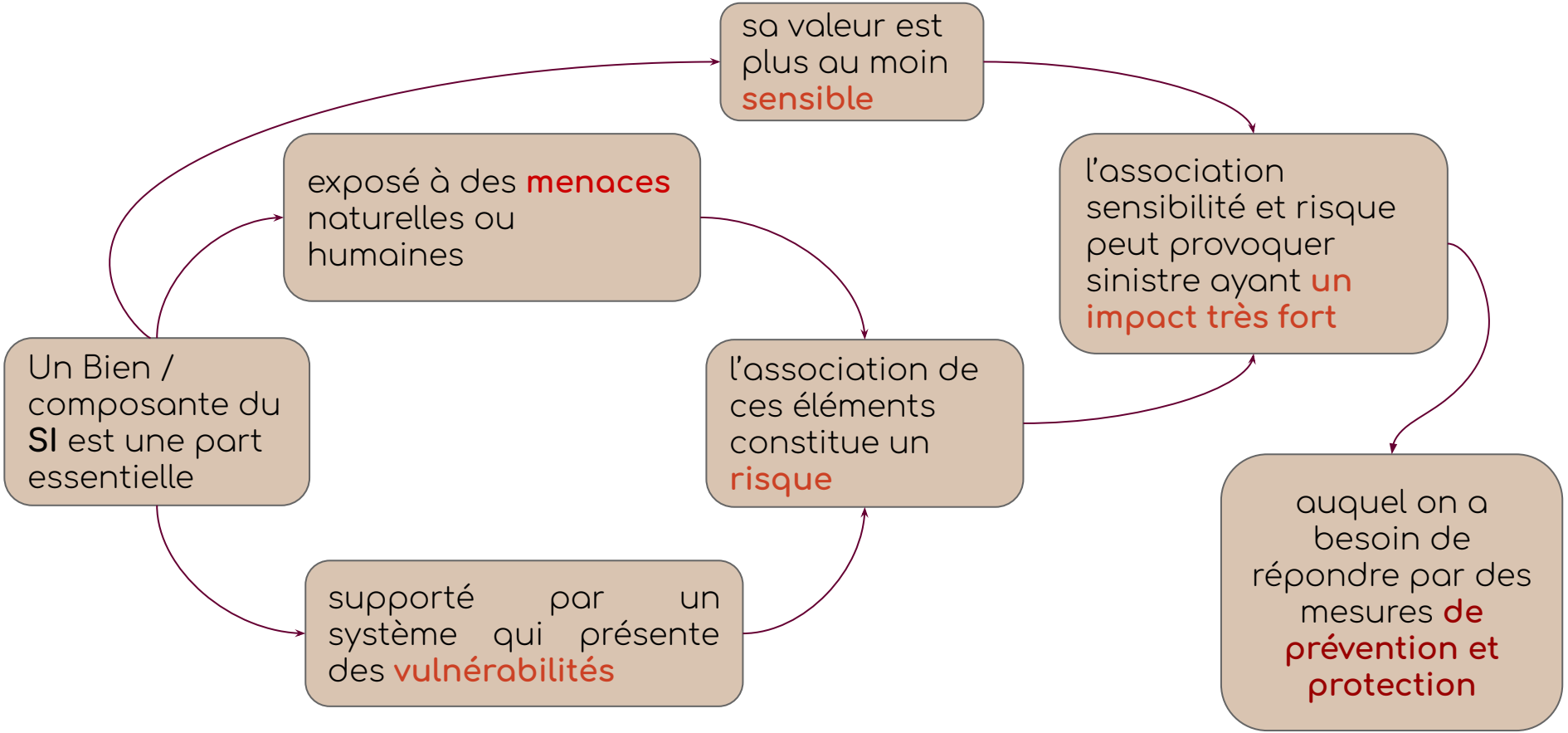
Tout événement intéressant la sécurité de l'information indésirables(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information

Mécanisme de sécurité

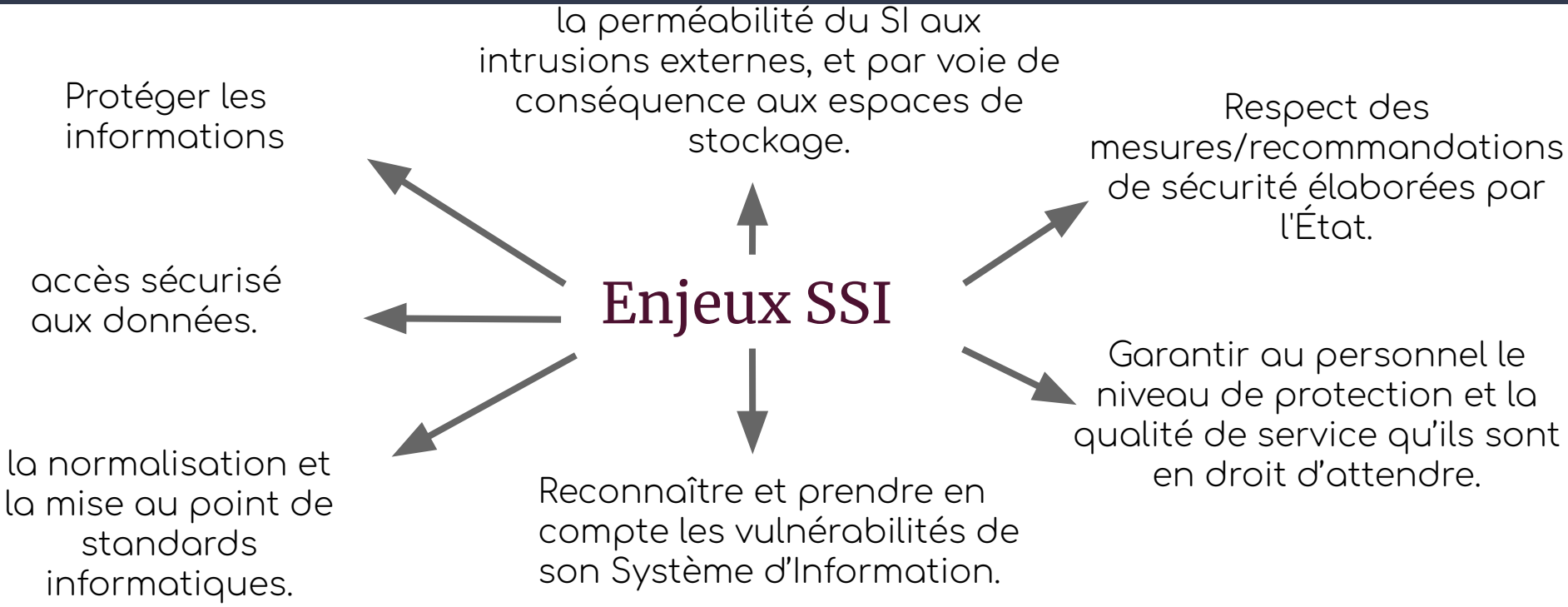
un processus (ou un périphérique incorporant un tel processus) conçu pour détecter, prévenir ou récupérer une attaque de sécurité.

Service de sécurité

Destinés à contrer les attaques de sécurité, et ils utilisent un ou plusieurs mécanismes de sécurité pour fournir le service


sa valeur est plus au moin sensible
l'association sensibilité et risque peut provoquer sinistre ayant un impact très fort
auquel on a besoin de répondre par des mesures de prévention et protection
l'association de ces éléments constitue un risque
supporté par un système qui présente des vulnérabilités
Un Bien / composante du SI est une part essentielle
exposé à des menaces naturelles ou humaines

Enjeux de la SSI



Comment sécuriser un SI

- ➔ Démarche générale de mise en oeuvre
- ➔ Principales mesures de protection

La démarche adopte **une spirale évolutive régulière** :

1. **Évaluer les risques et leur criticité**: quels risques et quelles menaces, sur quelles données et quelles activités, avec quelles conséquences ?

2. **Rechercher et sélectionner les parades**: que va-t-on sécuriser, quand et comment ? Étape difficile des choix de sécurité : dans un contexte de ressources limitées (en temps, en compétences et en argent)

3. **Mettre en œuvre les protections**

4. **Vérifier leur efficacité**

Méthodes d'analyse de risque

- **La méthode EBIOS** (Expression des besoins et identification des objectifs de sécurité), développée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ;

- **La méthode MEHARI** (Méthode harmonisée d'analyse des risques), développée par le CLUSIF ;

- **La méthode OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation), développée par l'Université de Carnegie Mellon (USA).

De nombreux moyens peuvent être mis en œuvre pour assurer une sécurité du système d'information. Il convient de choisir les moyens nécessaires, suffisants, et justes.

- **Systèmes de sauvegarde**: opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un SI (sauvegarde régulière quotidienne, hebdomadaire et autres)

- **Solutions de récupération des données:** opération informatique qui consiste à retrouver les données perdues à la suite d'une erreur humaine, une défaillance matérielle, une défaillance logicielle ...

- **Contrats d'assurance**: notamment contre l'impossibilité d'activité. La compagnie prend à sa charge de simuler financièrement une activité normale. Les assurances peuvent couvrir également les vols ou détériorations de matériel et de données.

Principales mesures de protection

- **Protection des locaux**: Construction des locaux étudiés (rangement des fils, goulottes pour les prises et les câbles réseaux).

- **Protection des matériels.** Dispositifs de continuité de l'alimentation électrique (onduleurs) ; dispositifs à tolérance de pannes au niveau des architectures matérielles et de communication; télésurveillance contre les intrusions malveillantes.

- **Protection des accès (contrôle d'accès)** .

Principales mesures de protection

- **Protection des échanges**. Instauration de serveurs de sécurité. Un serveur de sécurité est un dispositif matériel (nommé antéserveur) ou logiciel. Placés en amont ou en aval du système à sécuriser, ces serveurs permettent d'assurer certaines fonctions de sécurité: système d'authentification, contrôle d'accès, chiffrement, signature électronique, serveur de secours, outil d'audit, etc.

- **Le journal d'audit** est un outil précieux pour surveiller les accès. C'est un relevé de toutes les opérations effectuées sur le réseau. Il permet de se prémunir contre la non-répudiation (on sait "qui a fait quoi et même quand").

Principales mesures de protection

- **Définir une Politique de sécurité**: ensemble des orientations suivies par une entité en termes de sécurité. À ce titre, elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.

- **Sécuriser chaque sous-ensemble du système**, et s'oppose à la vision d'une sécurisation du système uniquement en périphérie. De façon puriste, les divers composants d'un SI ne font pas confiance aux autres composants avec lesquels ils interagissent. Ainsi, chaque composant effectue lui-même toutes les validations nécessaires pour garantir la sécurité.

Principales mesures de protection

Principales mesures de protection

- **Anti-virus**: Mécanisme technique permettant de détecter toute attaque virale qui a déjà été identifiée par la communauté sécurité

- **Contrôles d'accès logiques**: Mécanismes permettant de restreindre l'accès en lecture/écriture/suppression aux ressources aux seules personnes dument habilitées

- **Pare-feu**: Équipement permettant d'isoler des zones réseaux entre-elles et de n'autoriser le passage que de certains flux seulement

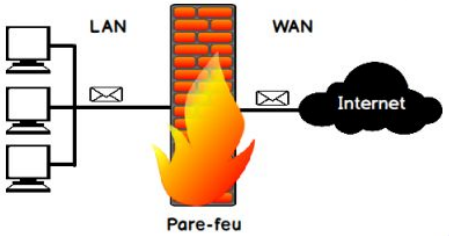
- ➔ **Capacité d'audit**: Mécanismes organisationnels destinés à s'assurer de l'efficacité et de la pertinence des mesures mises en œuvre. Participe à l'amélioration continue de la sécurité du S.I.

- ➔ **Clauses contractuelles avec les partenaires**: Mécanismes organisationnels destinés à s'assurer que les partenaires et prestataires mettent en œuvre les mesures nécessaires pour ne pas impacter la sécurité des S.I. de leurs clients

- ➔ **Formation et sensibilisation**: Mécanismes organisationnels dont l'objectif est d'expliquer aux utilisateurs, administrateurs, techniciens, PDG, clients, grand public, etc. en quoi leurs actions affectent la sécurité des S.I.

Principales mesures de protection

- **Le pare-feu** (firewall): est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique.



Niveau des adresses IP : faire accepter les flux de données provenant d'une plage d'adresses,
Niveau des noms de domaine : il est possible d'empêcher l'accès à certaines adresses Internet.
Niveau des protocoles : pour empêcher tout transfert FTP, Telnet, (HTTP).
Niveau des ports :
Niveau des mots ou phrases : semblable aux expressions régulières, il est possible de refuser les paquets dont le contenu renferme des séquences.

Principales mesures de protection

- ➔ stéganographie
- ➔ certificat
- ➔ fonction de hachage

Outils cryptographiques

Technique utilisée pour assurer la confidentialité des informations

Fondée sur des algorithmes mathématiques pour rendre les données illisibles pour les personnes non autorisées

- ➔ **La signature électronique**: Il s'agit d'informations ajoutées au pour donner une information supplémentaire permettant, soit de contrôler qu'il n'y a pas d'erreurs de transmission ou de rejet, soit de disposer d'une preuve non répudiante de l'envoi des données par l'émetteur.

- ➔ **Chiffrement**: codage des informations à l'aide d'un algorithme spécifique et d'une clé.

Principales mesures de protection

- ➔ **IDS (outil de détection d'intrusions)**: ce logiciel émet une alarme lorsqu'il détecte toute violation de privilège interne ou externe.

- ➔ **Programme teste de vulnérabilité:**

Principales mesures de protection

Menaces

- ★ Types de menaces
- ★ Principales menaces effectives
- ★ Panorama de quelques menaces

Menaces accidentelles

- Menace d'un dommage n**on intentionnel** envers le Système
- Elles ne supposent aucune préméditation.
- Dans cette catégorie, sont repris : les bugs logiciels, les pannes matérielles, Catastrophe naturelle

Menaces intentionnelles

- Elles reposent sur l'action d'un **tiers** désirant s'introduire et relever des informations.
- Elle est le fait d'un acte délibéré.
- Dans cette catégorie, sont repris : L'espionnage, Le vol, Le sabotage, La fraude physique

Types de menaces

- **Un utilisateur du système** : l'énorme majorité des problèmes liés à la sécurité d'un système d'information **est l'utilisateur (insouciant)** ;

- **Une personne malveillante** : une personne parvient à s'introduire sur le système, légitimement ou non, et à accéder ensuite à des données ou à des programmes auxquels elle n'est pas censée avoir accès en utilisant.

- **Un programme malveillant** : un logiciel destiné à nuire ou à abuser des ressources du système est installé, ouvrant la porte à des intrusions ou modifiant les données

- **Un sinistre (vol, incendie, dégât des eaux)** : une mauvaise manipulation ou une malveillance entraînant une perte de matériel et/ou de données.

Principales menaces effectives

Panorama de quelques menaces

- **Virus**
  un programme informatique malveillant dont l'objectif est de perturber le fonctionnement normal d'un système à l'insu de son propriétaire.tendent à devenir de plus en plus ciblés sur un secteur d'activité (Message avec pièce-jointe, Support amovible (clé USB...), Site Web malveillant ou piratés, Partages réseaux ouverts, systèmes vulnérables...

- **Cheval de Troie**
  Petit programme malveillant d'apparence anodine qui peut causer des dégâts une fois installé (virus classique, permettre de prendre le contrôle de l'ordinateur à distance). Les chevaux de Troie lisent les mots de passe, enregistrent les frappes ou ouvrent la voie à d'autres programmes malveillants qui peuvent même prendre en otage l'ordinateur tout entier. Ces actions peuvent être (Suppression/ Blocage/ modification) de données, Perturbation des performances des ordinateurs ou des réseaux informatiques

- **ver**
  est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet. Il a la capacité de se dupliquer une fois qu'il a été exécuté.
- **Spywares (Logiciels espions)**:
  agit comme son nom l'indique, à savoir, espionner ce que vous faites sur votre ordinateur. Il recueille des données telles que les saisies clavier, les habitudes de navigation et les informations de connexion qui sont alors envoyées à des tiers, généralement des cybercriminels. Il peut également modifier des paramètres de sécurité spécifiques sur un ordinateur
- **Botnets**:
  un ensemble de systèmes contrôlables par un attaquant via des serveurs de commande. Les propriétaires de ces systèmes ne savent pas que leur PC participe à un botnet (leur PC a été compromis au préalable et à leur insu via l'exploitation d'une vulnérabilité) .

Panorama de quelques menaces

Attaques

- ★ Catégorie d'attaques
- ★ Type d'attaques
- ★ Techniques d'attaques
- ★ Quelques profils d'attaquants

Catégorie d'attaques

Interception

- Attaque portée à la confidentialité.
- Il peut s'agir d'une personne, d'un programme ou d'un ordinateur.
- Une écoute dans le but de capturer des donn´ees sur un r´eseau,
- La copie non autorisée de fichiers ou de programmes.

interruption

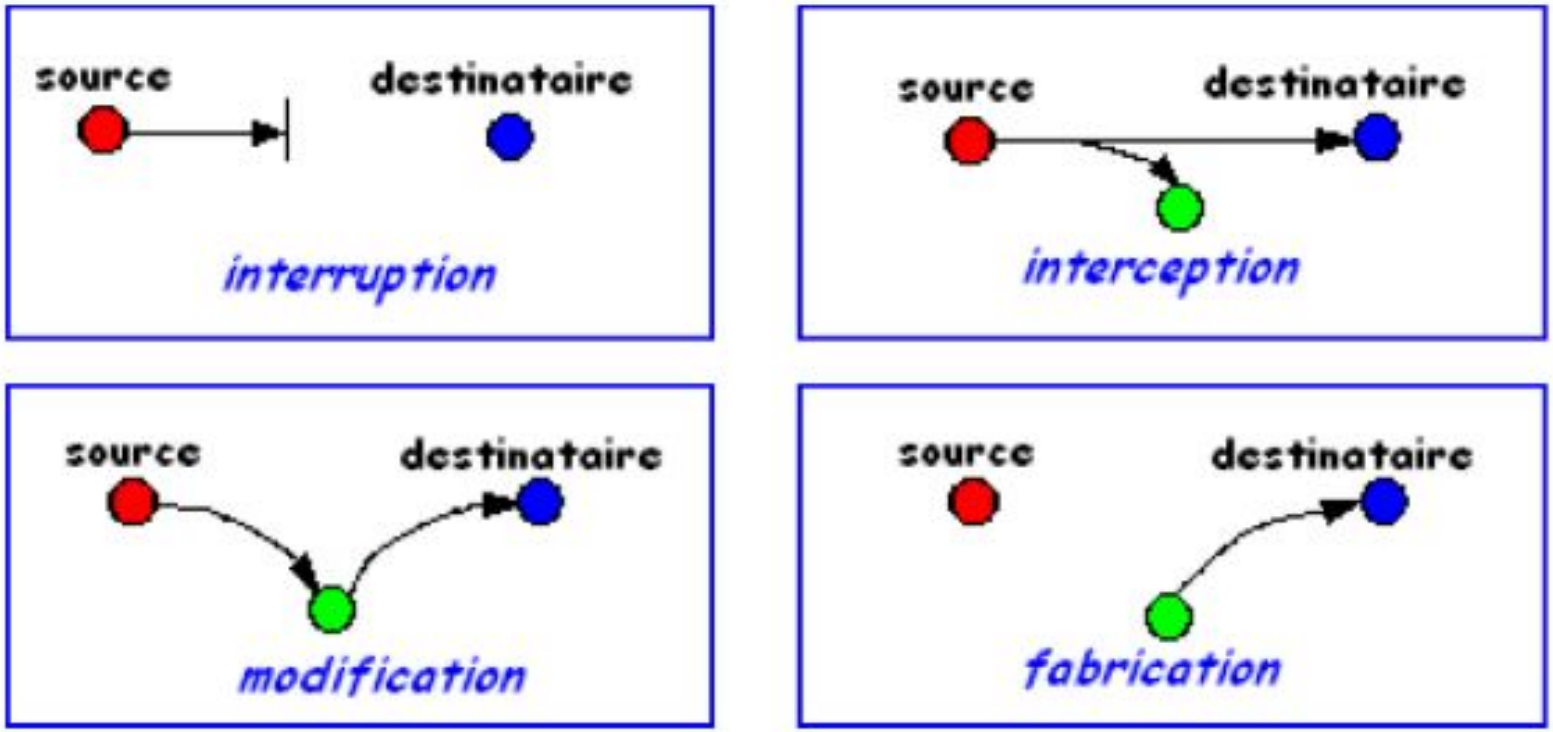
- C'est une attaque portée à la disponibilité, elle consiste à rendre les données d'un système inaccessible.
- Suppression de données, la destruction d'une pièce matérielle Mise hors service d'un système de gestion de fichiers.

Fabrication

C'est une attaque portée à l'authenticité.
Il peut s'agir de l'insertion de faux messages dans un r´eseau ou l'ajout d'enregistrements `a un fichier par une tierce partie non autoris´ee.

Modification

-Il s'agit d'une attaque portée à l'intégrité
- Changer des valeurs dans un fichier de données, altérer un programme de façon à bouleverser son comportement ou modifier le contenu de messages transmis sur un réseau.



Catégorie d'attaques

Type d'attaques

- Une attaque peut être classée par son **comportement** ou par **la position de l'attaquant**.

Comportement

Active: tente de modifier les ressources du système ou d'affecter leur fonctionnement

Passive: tente d'apprendre ou d'utiliser des informations du système mais n'affecte pas les ressources du système.

Position

Interne: attaque initiée par une entité dans le périmètre de sécurité. Une entité autorisée à accéder aux ressources du système mais qui les utilise d'une manière non approuvée par ceux qui ont accordé l'autorisation.

Extérieure : initiée depuis l'extérieur du périmètre, par un utilisateur non autorisé ou illégitime du système

➔ **Hameçonnage et ingénierie sociale** (anglais "phishing"):
vise à abuser de la "naïveté" des clients/employés pour:

- Dérober directement des informations confidentielles (leurs identifiants de banque en ligne ou leurs numéros de carte bancaire...
- Pour introduire des logiciels malveillants dans le système d'information de la banque

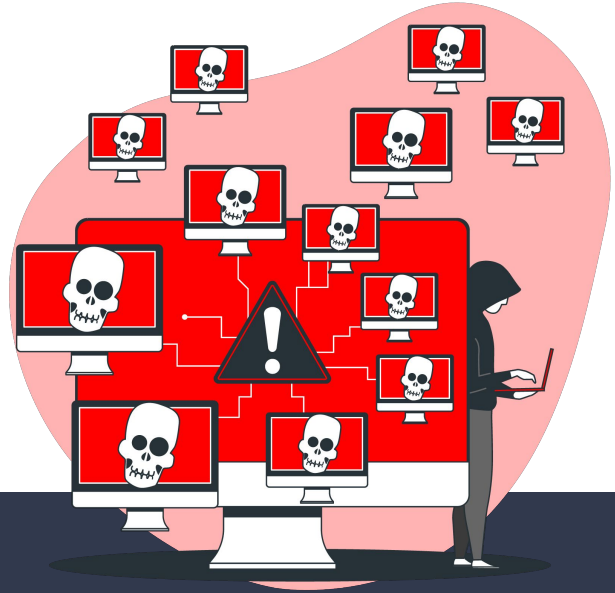
directement des informations confidentielle, ou

Techniques d'attaques

➔ Déni de service Distribué (DDoS)

Vise à perturber le bon fonctionnement d'un service.
Elle exploite les vulnérabilités logicielles existantes et non traitées.

Par exemple, envoyer 1.000.000 de requêtes en moins de 5 secondes à un serveur web avec des adresses IP sources fictives, constitue une attaque d type déni de service sur le serveur Web.



➔ **Attaque de l'homme du milieu (Man-In-The-Middle)**

Ce type d'attaque vise à intercepter les communications entre deux parties (personne, ordinateur) sans que ni l'une, ni l'autre ne puisse s'en apercevoir. Il s'agit ici d'une attaque par interception

➔ **Reniflage (sniffing)**

Cette technique consiste à écouter une ligne de transmission par laquelle transitent des données pour les récupérer à la volée.

Cette technique peut être utilisée à l'interne pour le débogage ou de manière abusive par un pirate cherchant, par exemple, à se procurer un mot de passe.

Vise surtout à intercepter les données non chiffrées.

➔ **Mystification (Spoofing)**

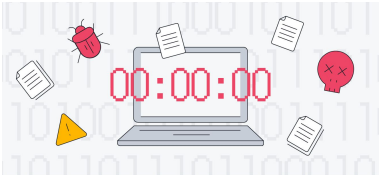
Technique d'intrusion consistant à envoyer à un serveur des paquets qui semblent provenir d'une adresse IP connue par le coupe-feu. La machine est rendue inatteignable par le pirate pour pouvoir intercepter les codes de communication et établir la liaison pirate.

Techniques d'attaques

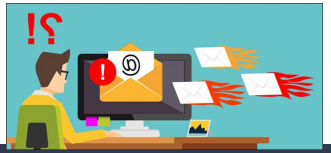
Techniques d'attaques

- **Porte dérobée (backdoor):** un point d'entrée dans un programme ou un système plus ou moins secret. Ǵeneralement une sécurité pour débloquer un code d'accès perdu ou pour le débogage. C'est aussi le point d'entrée des hackers. Ils peuvent même les créer pour les utiliser ultérieurement.

- **Bombe logique:** une fonction, cachée dans un programme en apparence honnête, utile ou agréable, qui se déclenche à retardement, lorsque aura atteint une certaine date, ou lors d'un certain événement. Cette fonction produira alors des actions ind´esir´ees, voire nuisibles



- **Spamming:** courrier indésirable est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantit´e effectu´es à des fins publicitaires ou de déni de service



Quelques profils d'attaquants

- **Pirate** : celui qui distribue et vend des logiciels protégés sous copyright

- **Hacker** : celui qui visite des ordinateurs qui ne lui appartiennent pas sans leurs causer des dommages mais pour personnaliser son système
  - **Les chapeaux noirs (black hats)** : ne respectent pas la loi, ils pénètrent par effraction dans les systèmes dans un intérêt qui n'est pas celui des propriétaires. L'intérêt **y est personnel**, généralement financier. Par exemple les créateurs de virus, de chevaux de Troie ou de logiciels espions.

  - **Les chapeaux blancs (white hats)** : les chapeaux blancs ont plutˆot comme ambition d'aider à la sécurisation du système, sans en tirer profit de manière illicite. Les chapeaux blancs bricolent et testent les systèmes d'information pour découvrir les vuln´rabilit´es pas encore connues ou non publiques.

  - **Les chapeaux gris (grey hats):** Il s'agit d'un hacker compétent, qui agit parfois avec l'esprit d'un un chapeau blanc, parfois avec celui d'un Un chapeau noir. Son intention n'est pas forcément mauvaise, mais il commet cependant occasionnellement un délit.

Quelques profils d'attaquants

- ➔ **Cracker** : celui qui veut casser un système et causer des Dommages
- ➔ **Script kiddies** : jeunes utilisateurs utilisant des programmes trouvés sur l'internet, pour vandaliser des systèmes informatiques afin de s'amuser
- ➔ **Social Engineer** : celui qui discute directement avec d'autres personnes en leur posant des questions afin de leurs soutirer des informations utilisées plus tard dans des attaques informatiques