digital lifelong learning

Certificat Exécutif en Cybersécurité

et Gouvernance des SI

Module 1 : Fondamentaux de la sécurité des SI

CHAPITRE 1

CONNAÎTRE LES CONCEPTS DE BASE DE LA SÉCURITÉ INFORMATIQUE

1. **Importance de la sécurité dans les SI**
2. Terminologie et définitions
3. Objectifs et propriétés de la sécurité
4. Quiz sur les notions de base de la sécurité informatique

Importance de la sécurité dans les SI

- Un système d'information contient généralement toutes les **informations sensibles** d'une entreprise, y compris les informations relatives à son fonctionnement, sa clientèle, ses produits, etc.
- Certaines attaques de sécurité visant les systèmes d'information peuvent causer une suppression, altération, falsification, ou diffusion des informations sensibles dont elles effectuent leurs traitements. Ce qui pourrait induire plusieurs risques graves à l'entreprise tel que pertes financières, perte de la confiance de sa clientèle, perte de son image de marque, etc.
- Par conséquent, la protection des systèmes d'information contre les attaques de sécurité est **primordiale**.
- La protection des systèmes d'information et leurs résistances aux attaques de sécurité permet à leur entreprise de :

  Garantir la protection des informations sensibles ;

  Assurer la continuité de ses activités et par conséquent préserver la confiance de ses clients ;

  Se protéger contre les risques potentiels.

01 - Connaître les concepts de base de la sécurité Informatique

Sécurité:

Ensemble des techniques qui assurent que les données et les ressources (matérielles ou logicielles) soient utilisées uniquement dans le cadre où il est prévu qu'elles le soient.

Système d'information:

Ensemble d'activités consistant à gérer les informations: acquérir, stocker, transformer, diffuser, exploiter…
Fonctionne souvent grâce à un system informatique

PARTIE 1

CHAPITRE 1

CONNAÎTRE LES CONCEPTS DE BASE DE LA SÉCURITÉ INFORMATIQUE

1. Importance de la sécurité dans les SI
2. **Terminologie et définitions**
3. Objectifs et propriétés de la sécurité
4. Quiz sur les notions de base de la sécurité informatique

01 - Connaître les concepts de base de la sécurité Informatique

Terminologie et définitions

Classification de la sécurité

- La sécurité fait référence à l'ensemble des outils, méthodes, et/ou techniques permettant de protéger des actifs contre des dommages potentiels et le rendre sûr.
- Différentes classes de sécurité peuvent être distinguées :

La sécurité de l'information : adresse la protection des informations (ou des données) dans **tous les processus de traitement de l'information** contre les dommages potentiels tel que la falsification, la suppression, ou la diffusion de l'information aux entités non autorisés.

La sécurité physique : se réfère au **contrôle de l'accès physique aux ressources matérielles et/ou logicielles** et à leurs protections contre les dommages physiques et le vol, grâce à l'utilisation des outils et/ou techniques de défense.

La sécurité informatique : adresse **la protection d'un système informatique** par la prévention, la détection et la réduction des conséquences des actions non autorisées exécutées par les utilisateurs (autorisés et/ou non autorisés). Elle adresse également la protection de l'information durant son traitement et son stockage.

La sécurité des communications : consiste à protéger :

- Les systèmes informatiques **connectés à un réseau de communication** (tel que le réseau internet).

- Les informations circulant **dans un réseau informatique** contre les dommages potentiels.

La sécurité opérationnelle : consiste à **protéger les opérations d'une organisation** pour empêcher les dommages potentiels visant les informations sensibles échangés (ou traités) durant une opération.

La sécurité opérationnelle se réfère à la mise en place des mesures de sécurité suite à un processus de gestion de risques.

Un processus de gestion de risque analyse les opérations d'une organisation du point de vue pirate, pour identifier les risques de sécurité.

PARTIE 1

01 - Connaître les concepts de base de la sécurité Informatique

Terminologie et définitions

Classification de la sécurité

- Partant des définitions précédentes, il est possible de noter que les quatre classes de sécurité (sécurité physique, sécurité informatique, sécurité des communications, et sécurité opérationnelle) sont indispensables pour assurer la sécurité de l'information. Par conséquent, ces quatre classes de sécurité peuvent être considérées comme sous-classes de la sécurité de l'information, comme illustré dans la figure suivante.

Les classes de la sécurité de l'information

PARTIE 1

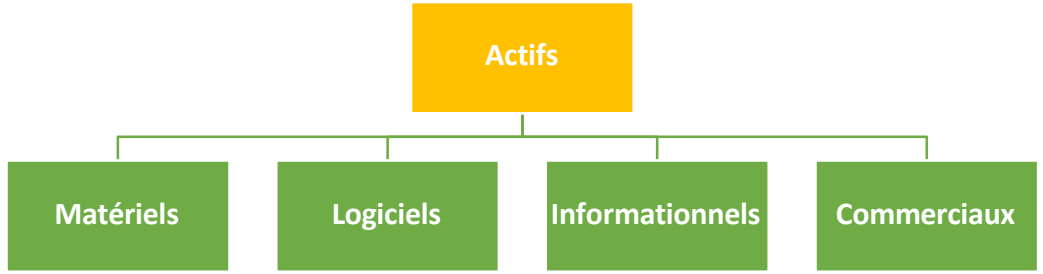
01 - Connaître les concepts de base de la sécurité Informatique

Terminologie et définitions

Actifs

- Un actif se réfère à tout ce qui a de la valeur pour une entité (une organisation ou une personne) et qui nécessite donc d'être protégé par des mesures de sécurité.
- Un actif peut être définit comme un bien, ayant la forme d'une donnée, appareil, ou composant, qui pourrait être consulté, utilisé, divulgué, détruit et/ou volé de manière illicite et entraîner une perte.
- Différent types d'actifs peuvent être distingués :
    - **Actifs matériels** : Ce sont les biens matériels qui exécutent des tâches spécifiques et/ou fournissent des produits. Les actifs matériels incluent des serveurs physiques, des postes de travail, des supports amovibles, des équipements de réseau, etc…
    - **Actifs logiciels** : Ce sont les bien logicielles qui exécutent des tâches de traitement des informations pour les transformer sous formes de données prêtes à être utilisées. Les actifs logiciels incluent les applications, les systèmes d'exploitation, les logiciels de virtualisation, les systèmes de gestion de base de données, les systèmes d'aide à la décision, etc…
    - **Actifs informationnels** : Ce sont les biens qui sont liés directement aux informations ou à leurs stockages, tels que les bases de données, les systèmes de fichiers, les informations de routage, etc…
    - **Actifs commerciaux** : Ce sont les autres biens d'une organisation qui ne rentrent pas dans les trois types d'actifs précédents (c.à.d., matériels, logiciels, et informationnels). Les actifs commerciaux incluent le capital humain, la réputation, l'image de l'organisation, etc…

Les types d'actifs



PARTIE 1

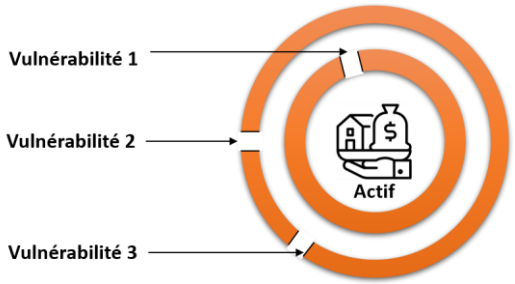
01 - Connaître les concepts de base de la sécurité Informatique

Terminologie et définitions

Vulnérabilité, Menace et Attaque

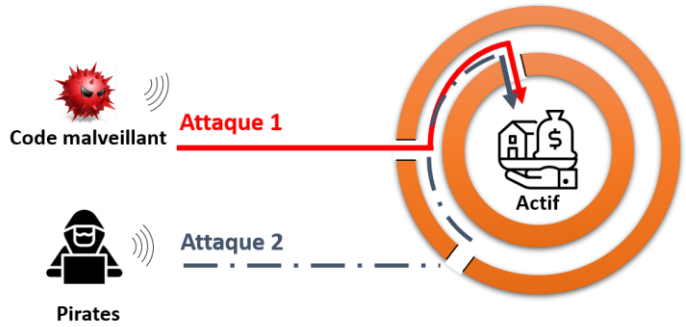
- **Vulnérabilité** : La faiblesse d'un actif (ou d'une ressource) l'expose à des menaces internes et externes pouvant entraîner des défaillances ou des violations. Les faiblesses peuvent être inhérentes à la conception, à la configuration, ou à la mise en œuvre d'un actif. Les mauvaises pratiques lors de l'utilisation d'un actif, tel que l'utilisation des mots de passes faibles pour accéder à cet actif, peuvent être aussi des sources de faiblesses.

Les vulnérabilités



- **Menace** : Un potentiel de violation de la sécurité qui pourrait exploiter une ou plusieurs vulnérabilités d'un actif pour l'endommager.

- **Attaque** : Une action ou un évènement non autorisée délibérée sur un actif pour causer son dysfonctionnement ou l'altération de l'information qu'il stocke.



PARTIE 1

01 - Connaître les concepts de base de la sécurité Informatique

Terminologie et définitions

Acteur de menace, Victime, Risque et Contre-mesures

- **Acteur de menace (Agent de menace)** : Une entité qui exécute et réalise une action de menace. Un agent de menace peut être :

  une personne ou groupe de personnes qui sont souvent des employés de l'entreprise ou des pirates ;

  un programme malveillant tel que les virus ; ou

  la nature lorsque la menace réalisée est une menace naturelle comme les tempêtes ou les inondations.

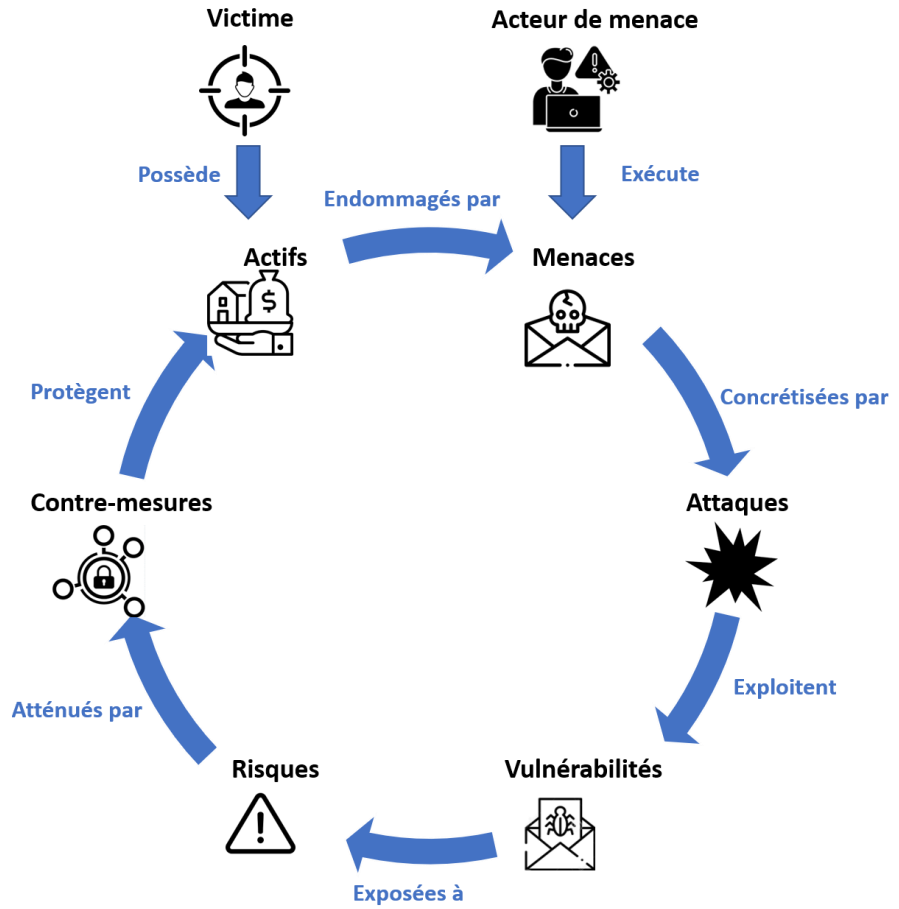
- **Victime** : La cible d'une attaque de sécurité. Elle est généralement une entité (une personne, groupe de personnes, organisations) qui possède un ou un ensemble d'actifs menacés par des attaques de sécurité.
- **Risque** : Une mesure qui évalue la combinaison du niveau de la gravité des conséquences de l'apparition d'une attaque de sécurité et la probabilité d'occurrence associée (c.à.d., la probabilité qu'une menace particulière exploite une vulnérabilité donnée).
- **Mesures de sécurité (Contre-mesures)** : Les techniques, méthodes, et/ou outils permettant la détection, la prévention ou la récupération des attaques de sécurité.

01 - Connaître les concepts de base de la sécurité Informatique

Terminologie et définitions

Terminologie et relations

- La figure suivante illustre les relations entre les différents termes qui ont été présentés précédemment. Ces relations sont détaillées ci-après
- Un acteur de menace exécute des menaces, qui sont généralement concrétisées par un ensemble d'attaques de sécurité, en exploitant des vulnérabilités.
- Les actifs qui souffrent de la présence des vulnérabilités sont exposés à des risques potentiels.
- Pour protéger les actifs contre les menaces de sécurité et atténuer les risques potentiels, il est possible de mettre en place un ensemble de mesures de sécurité (contre-mesures).
- Une victime est la cible d'une attaque. Elle possède des actifs qui pourraient être endommagés par des menaces de sécurité



Relations et terminologie de la sécurité

PARTIE 1

CHAPITRE 1

CONNAÎTRE LES CONCEPTS DE BASE DE LA SÉCURITÉ INFORMATIQUE

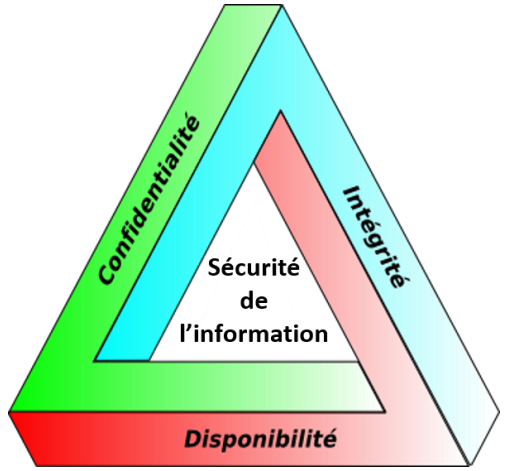
1. Importance de la sécurité dans les SI
2. Terminologie et définitions
3. **Objectifs et propriétés de la sécurité**
4. Quiz sur les notions de base de la sécurité informatique

01 - Connaître les concepts de base de la sécurité Informatique

Objectifs et propriétés de la sécurité

Disponibilité, Intégrité, Confidentialité (DIC)

- Pour assurer la sécurité de l'information, au moins les trois principaux objectives de la sécurité (souvent appelés triade DIC), que sont la disponibilité, l'intégrité et la confidentialité, doivent être atteints. La définition de ces trois objectives est fournie par la suite :
    - **Disponibilité** : exige qu'une ressource soit disponible et/ou fonctionnelle lorsqu' une entité autorisée la demande ;
    - **Intégrité** : exige que les actifs n'ont pas été modifié, détruit, falsifié, ou perdu d'une manière non autorisée ou accidentelle ;
    - **Confidentialité** : exige que les données ne soient pas divulguées aux entités à moins qu'elles n'aient été autorisées à accéder et à connaitre ces données.
- Lorsqu'un objectif de sécurité est assuré, il est souvent appelé propriété de sécurité.



La triade DIC pour la sécurité de l'information

Lien source

PARTIE 1

01 - Connaître les concepts de base de la sécurité Informatique

Objectifs et propriétés de la sécurité

Liste exhaustive des objectives de sécurité

- Une liste exhaustive d'objectifs relatifs à la sécurité de l'information comprend, en plus des objectives DIC, les éléments suivants :
    - **Authenticité** : exige d'être authentique et de pouvoir être vérifié, et digne de confiance. En d'autres termes, l'authenticité exige de vérifier que les identités fournies par les entités (utilisateurs ou processus) demandant accès à une ressource ne sont pas fausses et que ces entités sont bien ce qu'elles prétendent être ;
    - **Contrôle d'accès**: exige que l'accès à un actif ou une ressource soit contrôlée pour assurer que l'accès n'est possible que pour les entités autorisées ;
    - **Non-répudiation** : exige que les entités participantes à un évènement ou exécutant une action (tel que l'échange des messages , l'exécution des transactions, etc.) ne peuvent pas nier leur participation à cet évènement, ou l'exécution de cette action, respectivement. Cet objectif pourrait être atteint, en exigeant aux entités de fournir une preuve d'identité avant de participer à un évènement ou exécuter une action ;
    - **Traçabilité** : exige de suivre les actions exécutées par une entité durant son accès à un actif et de journaliser des informations décrivant les actions exécutées (tel que la durée d'accès, la nature des actions, les données utilisées, etc.) et que les actions exécutées peuvent être attribuées uniquement à cette entité, qui peut alors être tenue responsable de ses actions

CHAPITRE 1

CONNAÎTRE LES CONCEPTS DE BASE DE LA SÉCURITÉ INFORMATIQUE

1. Importance de la sécurité dans les SI
2. Terminologie et définitions
3. Objectifs et propriétés de la sécurité
4. **Quiz sur les notions de base de la sécurité informatique**

01 - Connaître les concepts de base de la sécurité Informatique

Quiz sur les notions de base de la sécurité informatique

Énoncé

- **Question 1 : Quelle est la propriété de sécurité qui garantie qu'un actif est accessible uniquement aux entités autorisées ?**
  - ❑ La confidentialité
  - ❑ L'intégrité
  - ❑ La disponibilité
  - ❑ L'authenticité
- **Question 2 : Quelle est la propriété de sécurité qui consiste à assurer qu'un actif devra répondre aux demandes des entités autorisées ?**
  - ❑ La confidentialité
  - ❑ L'intégrité
  - ❑ La disponibilité
  - ❑ L'authenticité
- **Question 3 : Un agent de menace peut être :**
  - ❑ Un employé
  - ❑ Un logiciel malveillant
  - ❑ Un pirate
  - ❑ Toutes les réponses sont correctes
- **Question 4 : Toutes les informations sensibles d'une organisation (tel que chiffre d'affaires, clientèle, produits, etc.) peuvent être considérées comme actif ?**
  - ❑ Vrai
  - ❑ Faux

CHAPITRE 2

IDENTIFIER LES ATTAQUES DE SÉCURITÉ VISANT UN SI

Ce que vous allez apprendre dans ce chapitre :

- Classifier les attaques de sécurité et les hackers
- Présenter les attaques internes et les attaques externes
- Mettre l'accent sur le besoin de l'identification des vulnérabilités

CHAPITRE 2

CONNAÎTRE LES CONCEPTS DE BASE DE LA SÉCURITÉ INFORMATIQUE

1. **Classification des attaques et des hackers**
2. Attaques internes
3. Attaques externes
4. Besoin d’identification des vulnérabilités

02 - Identifier les attaques de sécurité visant un SI

Classification des attaques et des hackers

Classification des pirates

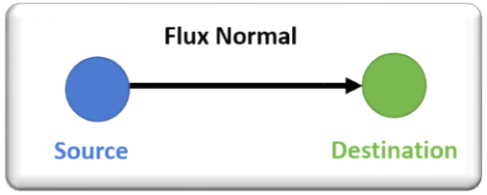
- Différents types de pirates peuvent être distingués selon leurs **niveau d'expertises** et/ou leurs intentions, lors de l'exécution des attaques :
    - **Les White hat hackers (les pirates chapeau blanc)** : ce sont souvent des **experts en sécurité** qui explorent en profondeur les systèmes d'information, afin de **découvrir les vulnérabilités** des ses systèmes et de les reporter aux responsables afin de les améliorer.
    - **Les Black hat hackers (les pirates chapeau noir)** : ce sont des pirates, qui ont des **mauvaises intentions** et dont la principale motivation est de **nuire aux systèmes d'information visés**
    - **Les Crackers** : ce sont des pirates dont la principale motivation est de **surmonter les outils de protections des logiciels payant**, grâce à des programmes logiciells (appelés souvent crack) développés. En effet, un crack permet de patcher un logiciel payant pour surpasser les protections mises en place.
    - **Les script-kiddies** : ce sont souvent **des pirates non experts en sécurité** qui réalisent leurs attaques de sécurité avec des outils et des logiciels existants. Les principales motivations de ces pirates sont **la destruction des systèmes d'information et le gain financier.**
    - **Hacktivistes** : ce sont des pirates dont la motivation principale est **idéologique**. Ils recourent généralement à l'attaque par déni de service. Anonymous est un exemples de Hacktivistes
- Après avoir classé les pirates, passons maintenant à la présentation des différentes classes d'attaques de sécurité qui peuvent être exécutées par les pirates.

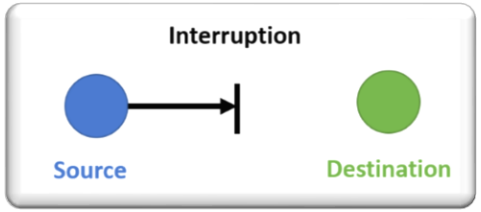
02 - Identifier les attaques de sécurité visant un SI

Classification des attaques et des hackers

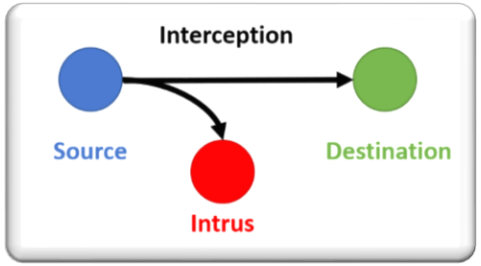
Classification des attaques

Les attaques de sécurité peuvent être classées en fonction de la propriété de sécurité visée. Quatre catégories d'attaques peuvent être distinguées : l'interruption, l'interception, la modification et la fabrication.

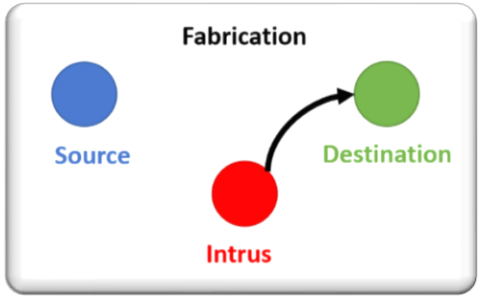




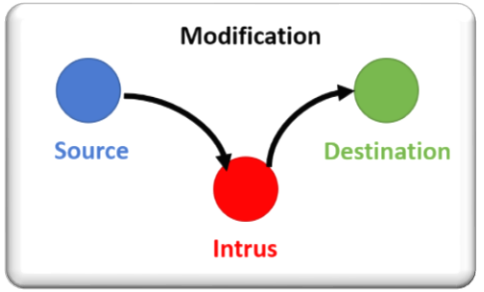
Un actif est détruit devient indisponible.
C'est une attaque qui vise la disponibilité.



Un intrus (une entité non autorisée) accède à un actif.
C'est une attaque qui vise la confidentialité.



Un intrus (une entité non autorisée) insère un faux objet dans un actif.
C'est une attaque qui vise l'authenticité.



Un intrus (une entité) non autorisée accède à un actif et le modifie.
C'est une attaque qui vise l'intégrité.

PARTIE 1

02 - Identifier les attaques de sécurité visant un SI

Classification des attaques et des hackers

Classification des attaques

- Un autre moyen de classification d'attaque de sécurité, qui a été utilisée à la fois dans **X.800** et **RFC 2828**, classifie les attaques de sécurité en fonction de leurs **effets sur les ressources visées**. Dans cette classification, deux classes d'attaques de sécurité sont distinguées : les attaques *passives* et les attaques *actives.*
- **Les attaques passives :**

  Dans ce type d'attaque, l'objectif de l'intrus est de collecter des informations concernant les ressources et les actifs sans réaliser aucune modification affectant l'information ou la ressource visée. Deux types d'attaques passives peuvent être distinguées, qui sont :

  La lecture du contenu des messages et **l'analyse du Traffic.**
- **Lecture du contenu des messages :**

  Ce type d'attaque est possible lorsque **le contenu des messages échangés** entre deux entités est un **texte en claire** (c.à.d., un texte non chiffré). Dans ce type d'attaque, l'intrus peut collecter et lire des messages (ou écouter une communication vocale) échangés entre deux entités (Alice et Bob, comme illustré dans la figure ci-dessous.).

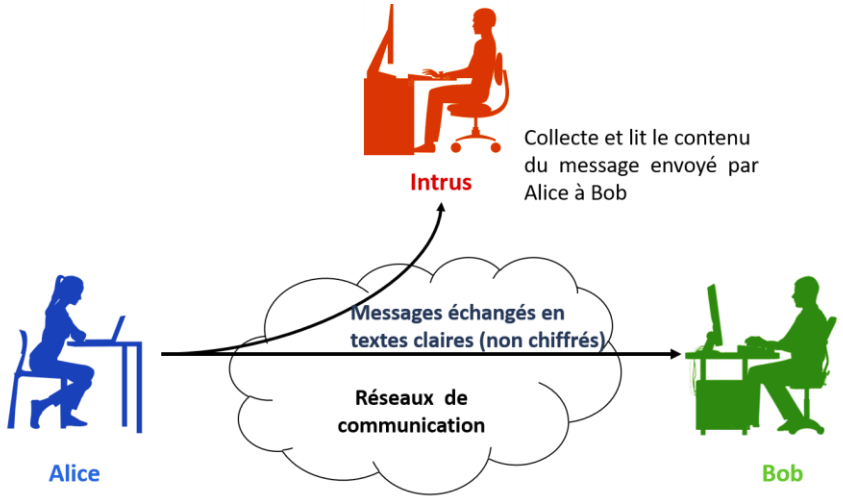


Illustration de l'exécution de l'attaque passive « lecture du contenu des messages »

PARTIE 1

Classification des attaques

Analyse du trafic : ce type d'attaque est exécuté lorsque **le contenu des messages échangés est masqué** (souvent en utilisant le cryptage). En fait, même en implémentant des mesures permettant de masquer le contenu des messages, l'intrus reste en mesure de collecter les messages, d'observer et d'analyser leurs structures, leurs motifs et/ou la fréquence des échanges. Le résultat de l'analyse lui permet de deviner la nature de la communication et d'exécuter d'autres attaques de sécurité plus sophistiquées.

Les attaques passives sont **difficiles à détecter**, puisqu'elles n'induisent aucune altération des données. Cependant, ce type d'attaques pourrait être **empêché** au moyen du **cryptage**. Par conséquent, le traitement des attaques passives doit être basé sur la prévention plutôt que sur la détection.

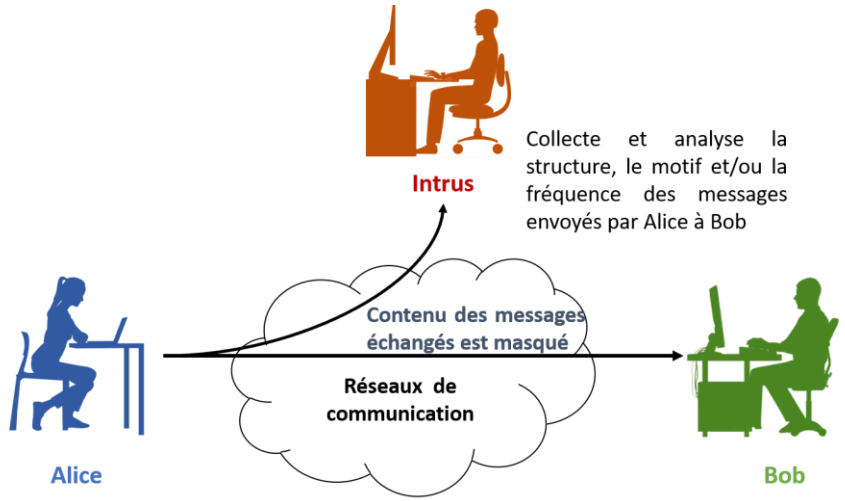


Illustration de l'exécution de l'attaque passive « Analyse du trafic»

PARTIE 1

02 - Identifier les attaques de sécurité visant un SI

Classification des attaques et des hackers

Classification des attaques

- **Les attaques actives** : Dans ce type d'attaque, l'objectif de l'intrus est de modifier les ressources et/ou d'affecter leur fonctionnement. Cela consiste souvent à une modification du flux de données ou à la création d'un faux flux. Quatre catégories d'attaques actives peuvent être distinguées : **mascarade, rejeu, modification des messages et déni de service.**

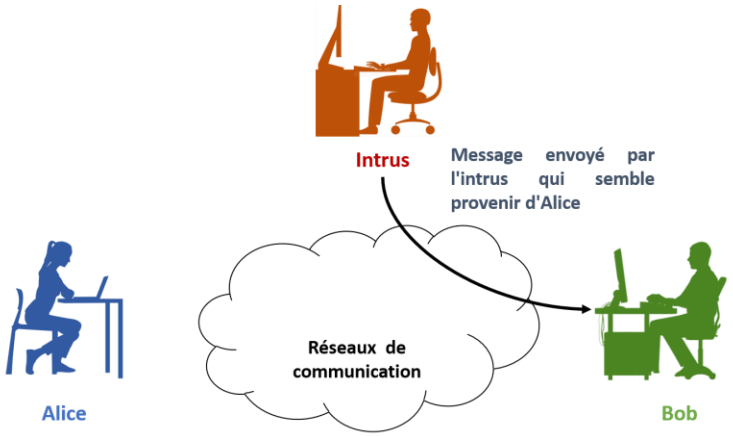


Illustration de l'exécution d'une attaque de mascarade

Mascarade : Cette attaque se réalise lorsqu'une entité fait semblant d'être une entité différente. Malgré le fait que le message reçu par Bob ait été envoyé par l'intrus, Bob croit que Alice est à l'origine du message.

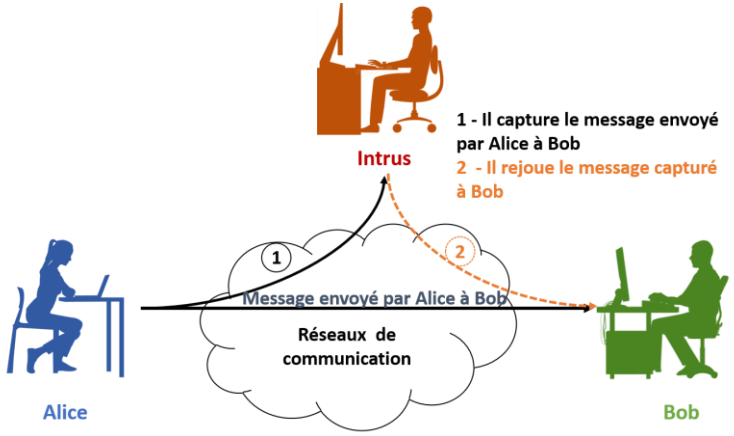


Illustration de l'exécution d'une attaque de rejeu

Rejeu : L'attaque de rejeu consiste à capturer une unité de données (ou un trafic de données) et la retransmet ensuite, sans effectuer aucune modification, pour réaliser un effet non autorisé. L'intrus exécute une attaque passive et capture le message envoyé par Alice à Bob. Par la suite, l'intrus renvoie le message capturé à Bob. L'exécution d'une attaque pourrait faire croire à Bob que ce message est envoyé par Alice.

PARTIE 1

02 - Identifier les attaques de sécurité visant un SI

Classification des attaques et des hackers

Classification des attaques

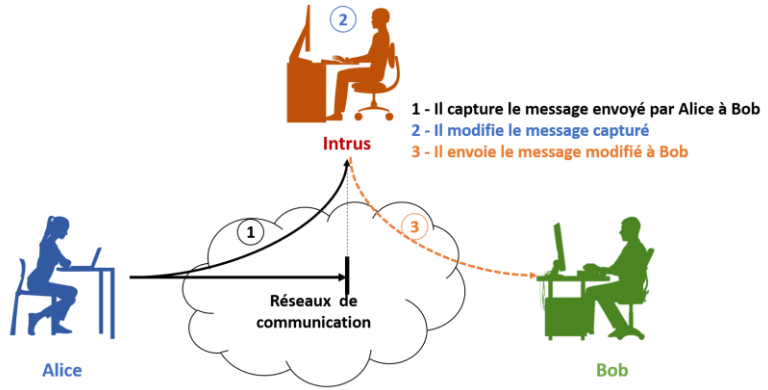


Illustration de l'exécution d'une attaque de modification des messages

Modification des messages : pour réaliser cette attaque, l'intrus modifie une partie d'un message capturé, ou retarde ou réorganise un ensemble de messages qui ont été capturés pendant une session légitime, pour produire un effet non autorisé.

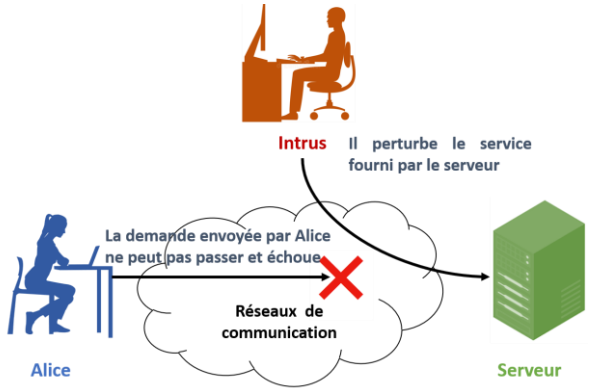


Illustration de l'exécution d'une attaque de déni de service

Déni de service : c'est une attaque qui pourrait se présenter sous plusieurs formes. Son objectif principal est d'empêcher ou d'entraver l'exécution des services visées. Exemples de formes d'attaques de déni de services :

- la suppression de tous les messages dirigés vers une destination particulière (le serveur dans notre exemple).
- la surcharge d'une destination particulière avec des faux messages pour dégrader ses performances et l'empêcher de répondre aux messages légitimes.
- l'interruption de l'ensemble du réseau (en le désactivant, le surchargeant, ou en provoquant une interférence) pour empêcher la réception des messages envoyés par des entités autoriséEs (la non réception du message d'Alice dans notre exemple).

PARTIE 1