



Sécurité Informatique

Chapitre I: Notions de base de la sécurité informatique

4^{ème} Année

Esprit 2022/2023



Plan du chapitre



- Les enjeux de la sécurité informatique
- Les métiers de la sécurité informatique
- Les objectifs de la sécurité informatique:
 - Confidentialité/Intégrité/Disponibilité/Authentification/Non-répudiation
- Terminologie de la sécurité informatique :
 - Vulnérabilité, menace/agent de menace, risque, impact, contre-mesure/protection.
- Règles de base de la sécurité informatique
- Lab : Mise en place de l'environnement de travail



Préambule (1/2)

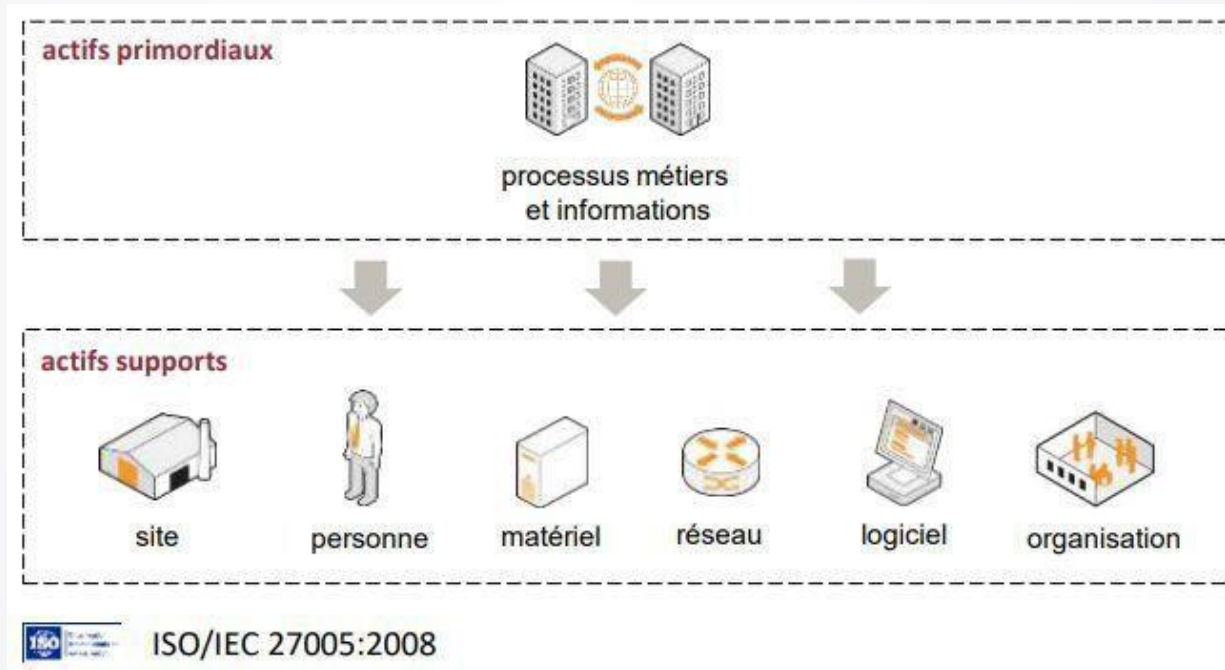


- Système Informatique
 - Des équipements informatiques: ordinateurs, serveurs, etc.
 - Des systèmes d'exploitation
 - Des applications et des logiciels
 - ...
- Ensemble des ressources destinées à: collecter, classifier, stocker, gérer, diffuser les informations au sein d'une organisation.
- Mot clé : **Information**, c'est le « **nerf de la guerre** » pour toutes les entreprises, administrations, organisations, etc.

Le S.I. doit permettre et faciliter la mission de

Préambule (2/2)

- Le système d'information d'une organisation contient un ensemble d'actifs :



La sécurité du S.I. consiste donc à assurer la sécurité de l'ensemble de ces biens



Les enjeux de la sécurité informatique



Objectifs de la sécurité informatique



- Réduire les risques pesant sur le système d'information, pour limiter leurs impacts sur le fonctionnement et les activités métiers des organisations...
- Les principaux objectifs de la sécurité informatique:
 - empêcher la divulgation non-autorisée de données
 - empêcher la modification non-autorisée de données
 - empêcher l'utilisation non-autorisée de ressources réseau ou informatiques de façon générale
- La gestion de la sécurité au sein d'un système d'information n'a pas pour objectif de faire de l'obstruction. Au contraire :
 - Elle **contribue** à la **qualité de service** que les utilisateurs sont en droit d'attendre
 - Elle **garantit** au personnel le **niveau de protection** qu'ils sont en droit d'attendre

► Pourquoi les pirates s'intéressent aux S.I? (1/3)



- Les motivations évoluent
 - Années 80 et 90 : beaucoup de bidouilleurs enthousiastes
 - De nos jours : majoritairement des actions organisées et réfléchies
- Cyber délinquance
 - Les individus attirés par l'appât du **gain**
 - Les « **hacktivistes** »
 - **Motivation** politique, religieuse, etc.
 - Les **concurrents** directs de l'organisation visée
 - Les **fonctionnaires** au service d'un état
 - Les **mercenaires** agissant pour le compte de commanditaires
 - ...



► Pourquoi les pirates s'intéressent aux S.I? (2/3)

- Gains financiers (accès à l'information, puis monétisation et revente)
 - Utilisateurs, emails
 - Organisation interne de l'entreprise
 - Fichiers clients
 - Mots de passe, N° de comptes bancaire, cartes bancaires
- Utilisation de ressources (puis revente ou mise à disposition en tant que « service »)
 - Bande passante & espace de stockage (hébergement de musique, films et autres contenus)
 - Zombies (botnets)
- Chantage/Vengeance
 - Il arrive que d'anciens employés attaquent leurs anciens employeurs par vengeance. Ce type d'intrus est particulièrement dangereux par sa connaissance intime du SI.

► Pourquoi les pirates s'intéressent aux S.I? (3/3)

■ Publicité

- Un intrus peut attaquer un réseau ou une application pour se faire connaître auprès du public ou pour se faire de la publicité pour ses propres services. Les intrus à la recherche de publicité font souvent état de leurs attaques.

■ Espionnage

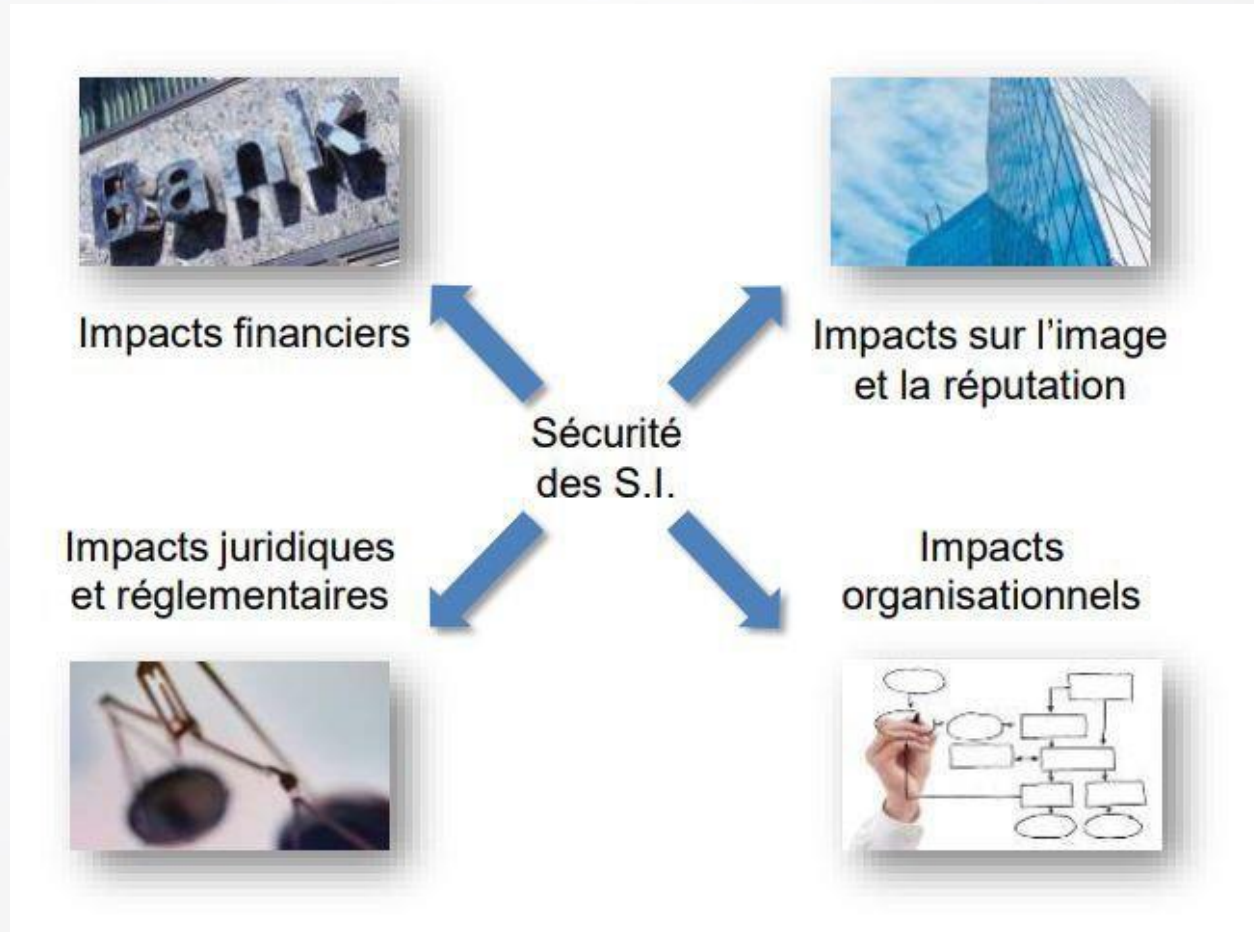
- Un intrus peut espionner une organisation ou un gouvernement afin d'obtenir des secrets. Ce type d'intrus est souvent motivé par le patriotisme ou l'appât du gain.

■ Terrorisme.

- Un intrus peut attaquer un réseau dans le cadre d'une opération de terrorisme d'état ou émanant d'un groupe. Il s'agit des types d'intrus les plus graves car il se peut que des vies humaines soient alors en danger.

Les intrus, quelles que soient leurs aptitudes et leurs motivations, sont dangereux pour la sécurité du système d'information

► Impacts de la Sécurité Informatique (1/2)



► Impacts de la Sécurité Informatique (2/2)

- Impact sur l'image / le caractère/ la vie privée
 - Diffamation / Harcèlement
 - Divulgence d'informations personnelles
- Usurpation d'identité
 - « Vol » et réutilisation de logins/mots de passe pour effectuer des actions au nom de la victime.
- Impacts financiers
 - N° carte bancaire usurpé et réutilisé pour des achats en ligne
 - Chantage (divulgence de photos ou d'informations compromettantes si non paiement d'une rançon).
- Perte définitive de données
 - Malware récents (rançongiciel) qui chiffre les données personnelles puis demande à leur propriétaire de payer une rançon contre en échange de la clé de déchiffrement.
 - Connexion frauduleuse à un compte « cloud » et suppression malveillante de l'ensemble des données



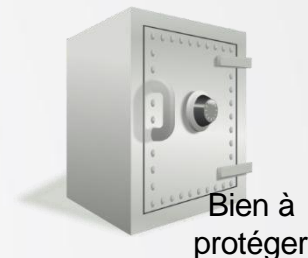
Les objectifs de la Sécurité Informatique

► Les critères D.I.C



Comment définir
le niveau de sécurité

Evaluer si le SI est
correctement sécurisé?



- **DIC**

- **Disponibilité:** Propriété d'accessibilité au moment voulu des biens par les personnes.
- **Intégrité:** Propriété d'exactitude et de complétude des biens et informations (i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée)
- **Confidentialité:** Propriété des biens de n'être accessibles qu'aux personnes autorisées.

► Critères complémentaires



• Besoins Complémentaires

- **La preuve:** Propriété d'un bien permettant de retrouver, avec **une confiance suffisante**, les circonstances dans lesquelles ce bien évolue. Cette propriété englobe notamment :
- **L'authentification:** Avoir l'assurance de l'identité d'une personne (ou d'un serveur) avec qui on échange
- **La non répudiation:** Avoir l'assurance que l'expéditeur d'un document ne puisse nier l'avoir envoyé ou que le destinataire ne puisse nier l'avoir reçu
- **L'horodatage:** Avoir l'assurance de la date et l'heure de l'exécution d'une action (envoi, réception, signature, ...) sur un document

► Sûreté vs Sécurité



« Sûreté » et « Sécurité » ont des significations différentes en fonction du contexte.

L'interprétation de ces expressions peuvent varier en fonction de la sensibilité de chacun.

Sûreté

- Protection contre les **dysfonctionnements** et **accidents involontaires**
 - Exemple de risque : saturation d'un point d'accès, panne d'un disque, erreur d'exécution, etc.
 - **Quantifiable statistiquement** (ex. : la durée de vie moyenne d'un disque est de X milliers d'heures)
- Ensemble de mécanismes mis en place pour assurer la continuité de fonctionnement du système.

Sécurité

- Protection contre les **actions malveillantes volontaires**
 - Exemple de risque : blocage d'un service, modification d'informations, vol d'information
 - **Non quantifiable statistiquement** , mais il est possible **d'évaluer en amont le niveau du risque et les impacts**.
- Ensemble de mécanismes destinés à protéger l'information des utilisateurs ou processus n'ayant pas l'autorisation de la manipuler et d'assurer les accès autorisés.

Exemple d'évaluation DICP



Auditer le niveau de
Disponibilité,
Intégrité,
Confidentialité et
de Preuve pour le
bien

Evaluer
ces
critères
sur une
échelle

Déterminer si ce
bien est correctement
sécurisé

- L'expression du besoin attendu peut-être d'origine
 - **Interne** : inhérente au métier de l'entreprise
 - **externe** : issue des contraintes légales qui pèsent sur les biens de l'entreprise.

Exemple



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

► Actions de Sécurité à mettre en place

Un Système d'Information a besoin de mécanismes de sécurité qui ont pour objectif d'assurer de garantir les propriétés DICP sur les biens de ce S.I.

Techniques : les solutions matérielles et logicielles

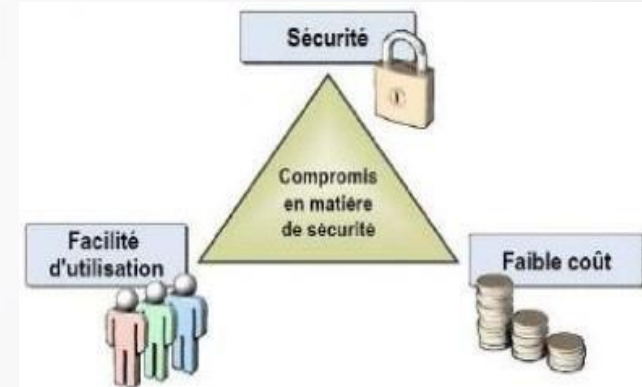
- Antivirus, Antispam, Firewall, contrôleur d'accès, etc.

Humains

- Direction informatique: Assure le bon fonctionnement des

Organisationnels

- Etablissement de la politique et l'organisation de la sécurité.



Mécanismes de Sécurité pour atteindre les besoins DICP

(1/2)

Exemples de mécanismes de sécurité

		D	I	C
		P		
Anti-virus	Mécanisme technique permettant de détecter toute attaque virale qui a déjà été identifiée par la communauté sécurité	✓	✓	✓
Cryptographie	Mécanisme permettant d'implémenter du chiffrement et des signatures électroniques		✓	✓
Pare-feu	Équipement permettant d'isoler des zones réseaux entre-elles et de n'autoriser le passage que de certains flux seulement	✓ ✓		✓
Contrôles d'accès logiques	Mécanismes permettant de restreindre l'accès en lecture/écriture/suppression aux ressources aux seules personnes dûment habilitées	✓	✓	✓
Sécurité physique des équipements et locaux	Mécanismes de protection destinés à protéger l'intégrité physique du matériel et des bâtiments/bureaux.	✓	✓	✓

Mécanismes de Sécurité pour atteindre les besoins DICP

(2/2)

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.

D
I
C
P

✓
✓

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. Diffusion des bonnes pratiques de sécurité.

✓
✓

Le cours actuel en est une illustration !



Terminologie de la Sécurité Informatique

An abstract geometric pattern consisting of various triangles in red, grey, and white, arranged in a dynamic, non-repeating composition. The triangles vary in size and orientation, creating a sense of movement and depth.

Me
nac
e

Impact

Attas

Con- tre- mes- ures

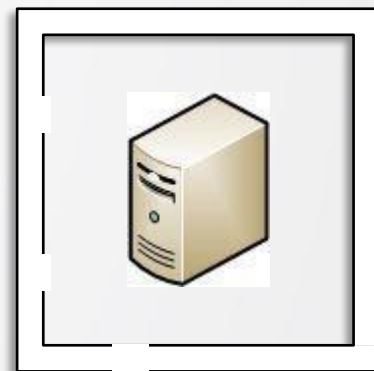
eent
aonutu
um e
fchan
ges ✓
peou
rquels
agatif
son
mrtut
amtu
canfa
nonh
theux
rosi
nich
séc
pu
• um m
égats
nuch
• tyou
Surtib
reana
elle
ellen
gner
lmpie
sante
e yai
dend
pact
enun
reelr
aufat

• Changement
• négatif
• le
• niveau
• des
• objectifs
• métiers
• atteints

► Les principales causes des vulnérabilités



Types de vulnérabilité	Exemple
Matériel	Maintenance insuffisante, absence de programme de remplacement périodique
Logiciel	Tests de logiciel absents ou insuffisants, interface utilisateur compliquée
Réseau	Connexions au réseau public non protégées, point de défaillance unique
Personnel	Formation insuffisante à la sécurité, travail non surveillé d'une équipe extérieure ou de l'équipe d'entretien
Site	Réseau électrique instable, emplacement situé dans une zone sujette aux inondations
Organisme	Absence de bonne attribution des responsabilités en sécurité de l'information, absence de responsabilités en sécurité de l'information dans les descriptions de postes

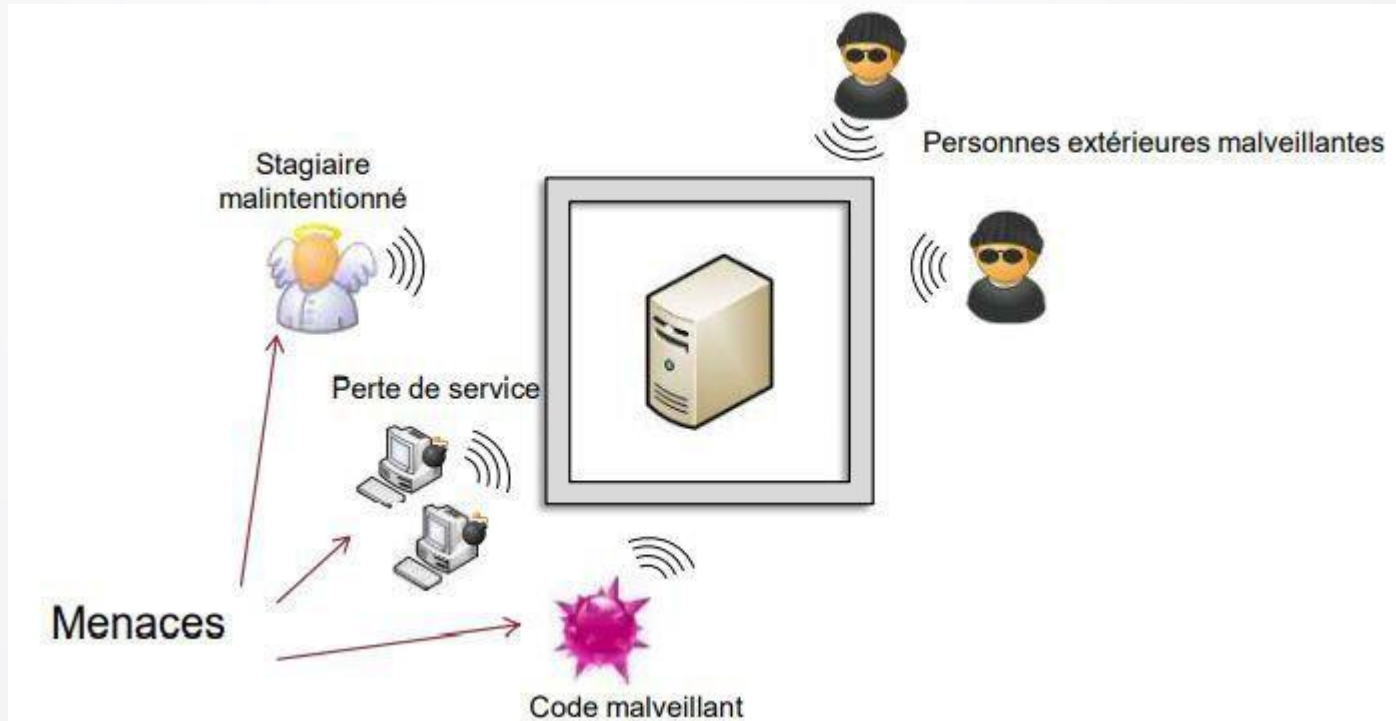


Vulnérabilités

► La menace (1)



- **Cause potentielle d'un incident**, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.



► La menace (2)



- Cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme
- Une menace est susceptible d'endommager les actifs tels que des informations, des processus et des systèmes et, par conséquent, des organismes. Les menaces peuvent être d'origine naturelle ou humaine et peuvent être accidentelles ou délibérées. Il convient d'identifier les sources de menaces à la fois accidentelles et délibérées

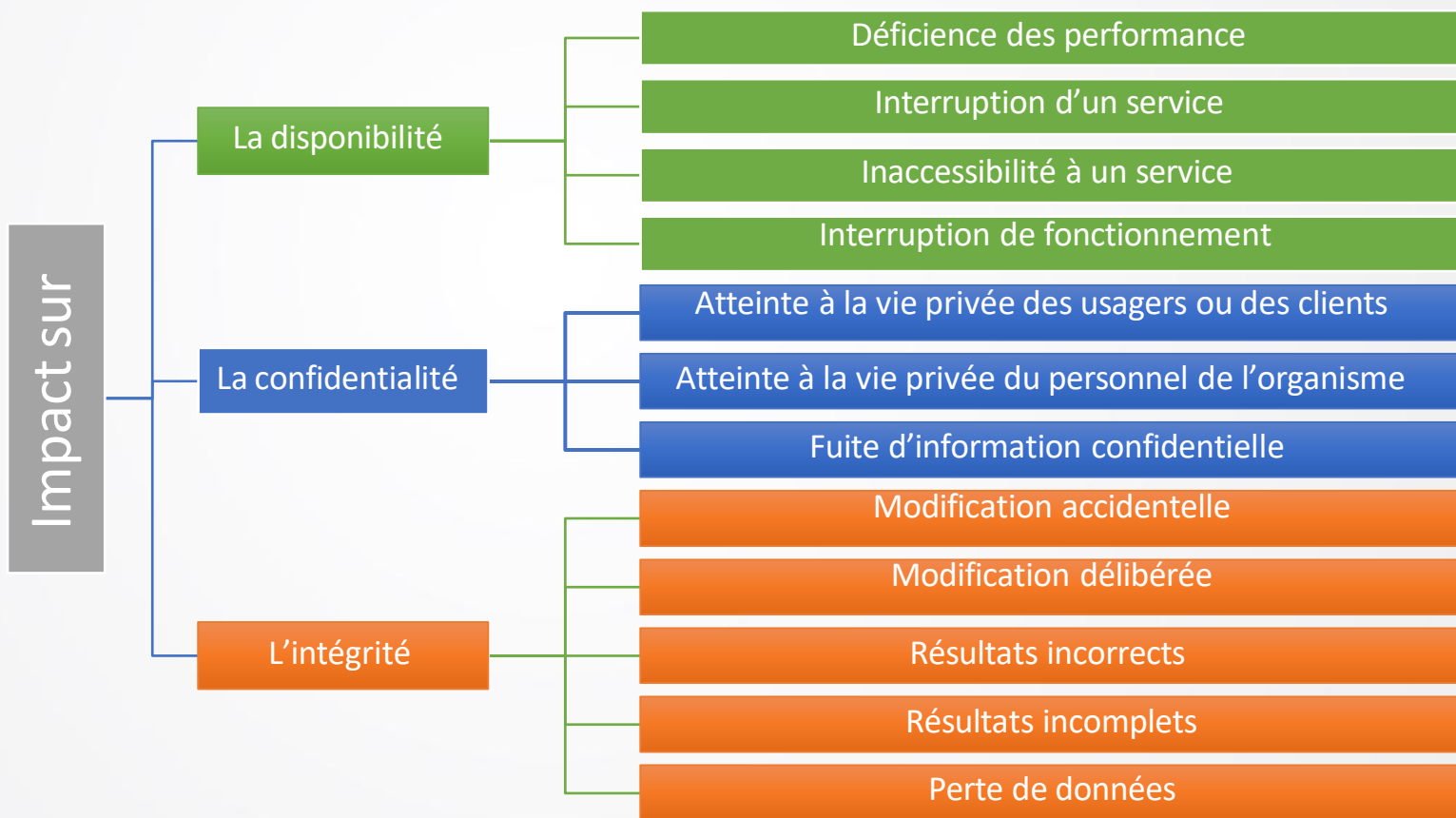


ISO/IEC 27000, clause 3.74 & ISO/IEC 27005, clause 8.2.3

L'impact



Changement négatif pénalisant le niveau des objets métier atteints



► Relation vulnérabilité-menace-impact

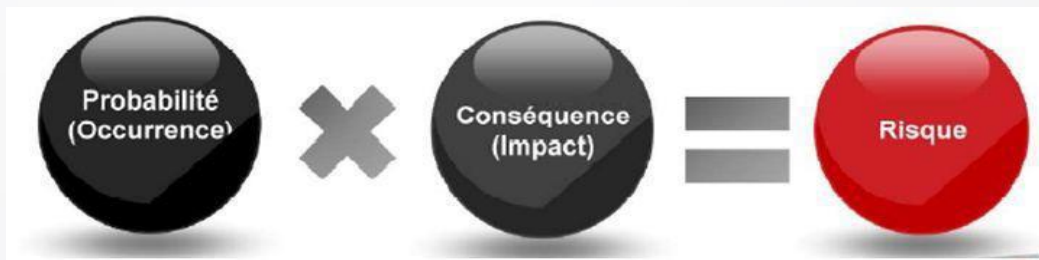



Vulnérabilité	Menace	Impact
Entrepôt sans surveillance	Vol d'équipement	Pertes financière
Interface utilisateur compliquée	Erreur de saisi de données	Base de données corrompue
Ligne de communication non protégée	Ecoute électronique	Interception des communications
Transfert des mots de passe en clair	Hacker	Vol d'information
Absence de processus de gestion des documents	Corruption des données	Documentation obsolète
Sensibilité à l'humidité	Corrosion	Echec de l'équipement

► Les Risques (1/3)



- Combinaison d'une menace et des pertes qu'elle peut engendrer
- La potentialité de l'exploitation de vulnérabilité par un élément menaçant et son impact sur l'organisme.
- Utile pour évaluer la probabilité d'un type d'incident donné
- Afin de réduire le danger à des niveaux acceptables, c'est-à-dire pour assurer la protection, il faut:
 - Réduire les menaces
 - Réduire les facteurs de vulnérabilité,
 - Augmenter les capacités de protection.





► Les Risques - Classification (2/3)

Vital : La nature du risque peut mettre en cause la survie de l'entreprise

Critique : La nature du risque peut affecter durablement les performances économiques de l'entreprise

Sensible : La nature du risque peut affecter l'entreprise de manière non négligeable même si limitée dans le temps.

Non critique : coût lié au risque existant mais limité

Risques humains

- La maladresse: erreurs, action non souhaitée, effacement involontaire des données, ...
- L'ignorance: introduire des programmes malveillants sans faire attention
- La malveillance: introduire des virus, ajouter des fonctions cachées, ...
- 1 cybercriminalité
- L'ingénierie social: informations personnelles confidentielles pour des fins suspectes
- L'espionnage

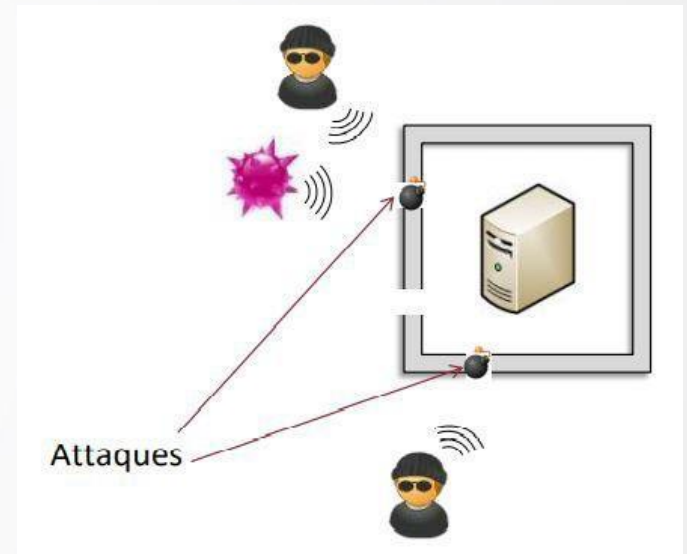
Risques logistiques

- Défauts et pannes de fabrication
- Panne matérielle
- Défaut du logiciel: système d'exploitation, programmes, etc.
- Environnement de travail: variation de la température ou l'humidité, exposition aux champs électriques et magnétiques

► Les attaques: Définition (1/4)

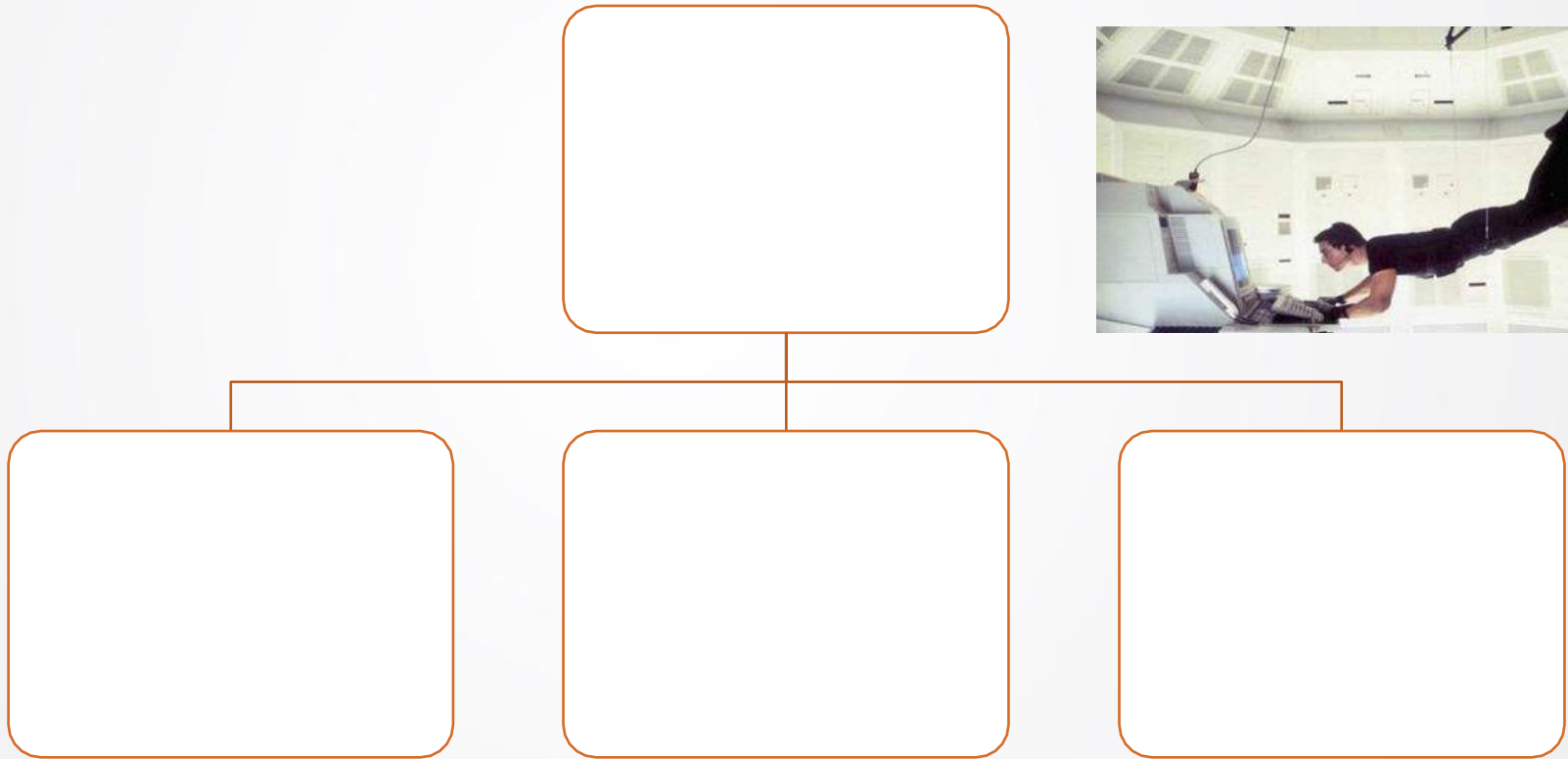


- **Action malveillante** destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la **concrétisation d'une menace**, et nécessite **l'exploitation d'une vulnérabilité**.
- Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité



Ainsi, tout le travail des experts sécurité consiste à s'assurer que le S.I. ne possède aucune vulnérabilité. Dans la réalité, l'objectif est en fait d'être en mesure de maîtriser ces vulnérabilités plutôt que de viser un objectif 0 inatteignable.

► Les attaques: l'attaquant (2/4)





► Attaque par logiciel malveillant (1)

- **Le virus** se duplique automatiquement sur le même dispositif et se transmet à un autre dispositif par l'intermédiaire du courrier électronique ou par l'échange de données
- **Le ver (*worm*)** exploite des communications réseaux d'une entité afin d'assurer sa reproduction sur d'autres dispositifs
- **Le cheval de Troie (*trojan*)** a une apparence légitime et exécute des routines nuisibles sans l'autorisation de l'utilisateur
- **La porte dérobée (*backdoor*)** permet d'ouvrir d'un accès réseau frauduleux sur un système informatique et peut exploiter à distance la machine



Attaque par logiciel malveillant (2)



- **Le logiciel espion (*spyware*)** fait la collecte d'informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation et les transmet à un ordinateur tiers
- **L'enregistreur de frappe (*keylogger*)** est généralement invisible, installé sur le poste d'un utilisateur et chargé d'enregistrer à son insu ses frappes clavier
- **L'exploit** permet d'exploiter une faille de sécurité d'un logiciel
- **Le rootkit** est un ensemble de logiciels permettant généralement d'obtenir les droits d'administrateur sur une machine, d'installer une porte dérobée, de truquer les informations susceptibles de révéler la compromission, et d'effacer les traces laissées par l'opération dans les journaux système.



Attaque par messagerie électronique



- **Le pourriel (*spam*)** est un courrier électronique non sollicité (publicité) qui encombre le réseau, et fait perdre du temps aux destinataires
- **L'hameçonnage (*phishing*)** est un courrier électronique dont l'expéditeur se fait généralement passer pour un organisme financier et demandant au destinataire de fournir des informations confidentielles
- **Le canular informatique (*hoax*)** est un courrier électronique incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes. Il encombre le réseau et incite l'utilisateur à effectuer des manipulations dangereuses sur son poste (suppression d'un fichier prétendument lié à un virus, ...).



Attaque par mise en réseau



- **les écoutes (*sniffing*)** permettent de récupérer toutes les informations transitant sur un réseau (par un logiciel *sniffer*)
 - récupérer les mots de passe des applications et identifier les machines communiquant sur le réseau.
- **L'usurpation d'identité (*spoofing*)** prend l'identité d'une autre personne ou d'une autre machine pour collecter des données sensibles, confidentielles, ...
- **Le déni de service (*denial of service*)** provoque des interruptions de service pour empêcher le bon fonctionnement d'un système
 - 1 Des tentatives d'extorsion de fond : menacer de stopper l'activité d'une entreprise.

► Les contre-mesures (1)



Superposition

- Une sécurité en couches, plus difficile à percer, résister à une variété d'attaques

Limitation

- Autorisation requise pour l'accès (limité, réduit).

Diversité

- Différenciation des couches de sécurité 1différenciation des outils d'attaque
- Violation d'une couche de sécurité \neq ensemble du SI.

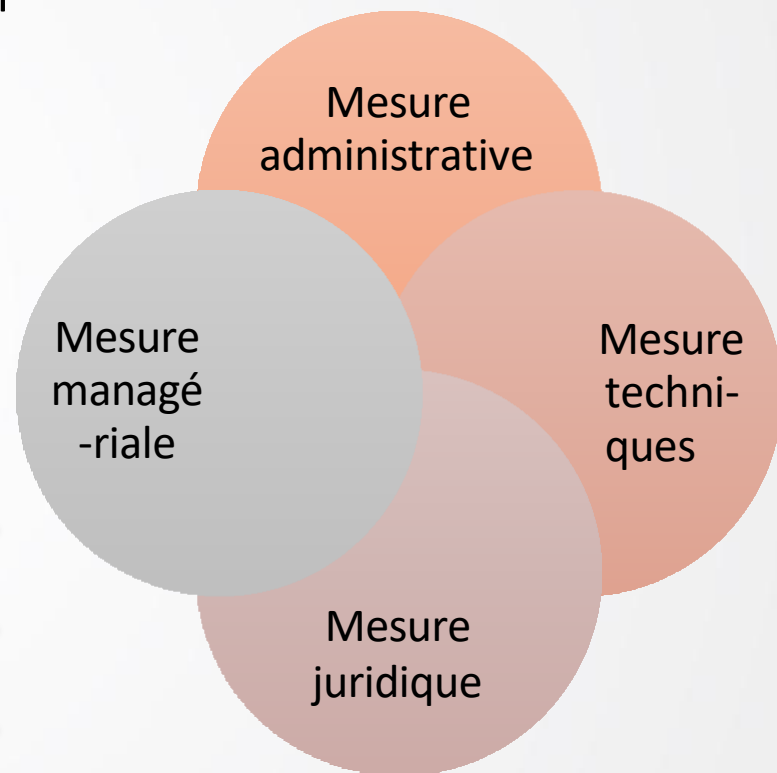
Obscurité

- Limiter les informations concernant un SI

► Les contre-mesures 2/2

- **Objectif d'une mesure de sécurité:** déclaration décrivant ce qui est attendu de la mise en œuvre des mesures de sécurité
- **Mesure de sécurité:**
 - Mesure qui modifie un risque
 - Les mesures de sécurité comprennent tous les processus, politiques, dispositifs, pratiques ou autres actions qui modifient un risque

Mesure préventive	Dissuader ou prévenir l'apparition de problèmes
Mesure de détection	Rechercher, détecter et identifier les anomalies
Mesure correctives	Remédier aux problèmes découverts et prévenir la répétition des anomalies



Relation entre concepts de sécurité

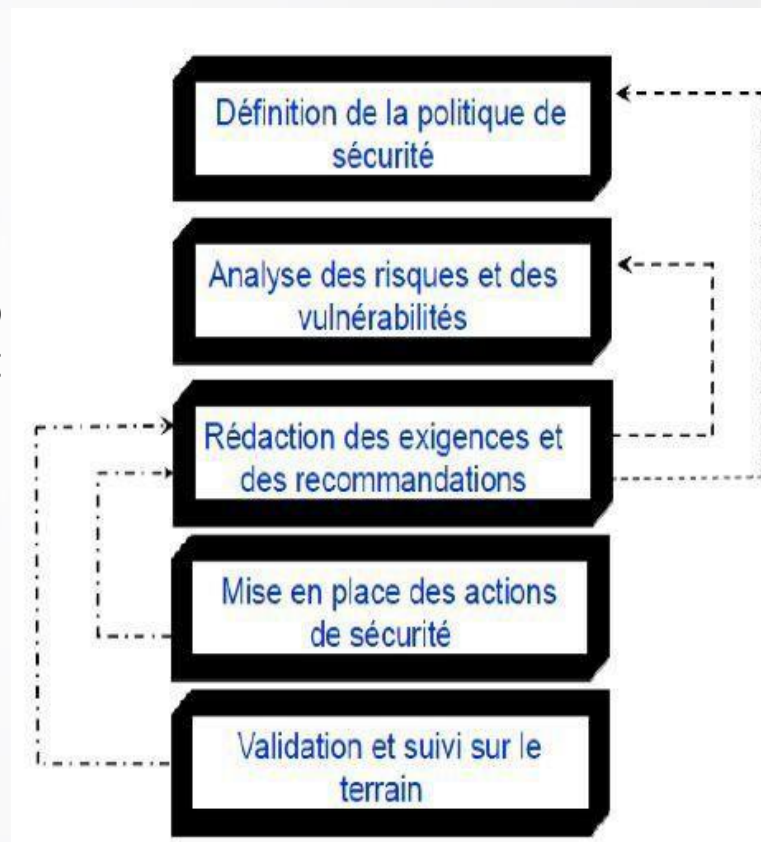




Règles de base de la sécurité informatique

► Méthodologie de la sécurité

1. Identifier la menace
 - Qui ou quoi / Comment (vulnérabilités) ?
2. Évaluer les risques et les vulnérabilités
 - Probabilité / Impact
3. Considérer les mesures de protection par rapport au risque
 - Efficacité / Coût / Difficulté d'utilisation
4. Mettre en place et opérer les mesures de protections
 - Modification et/ou installation
 - Changer les politiques
 - Éduquer les utilisateurs
5. Auditer, Valider et suivre





Règles de base



Interdiction par défaut	Tout ce qui n'est pas autorisé explicitement est interdit
-------------------------	---

Moindre privilège	N'autoriser que le strict nécessaire
-------------------	--------------------------------------

Défense en profondeur	Protection au plus tôt et à tous les niveaux
	Défenses en série

Goulet d'étranglement	Point de sortie unique permettant le contrôle
-----------------------	---

Simplicité	Filtrage le plus simple possible
------------	----------------------------------

Concertation	Acceptation des contraintes par utilisateurs
--------------	--

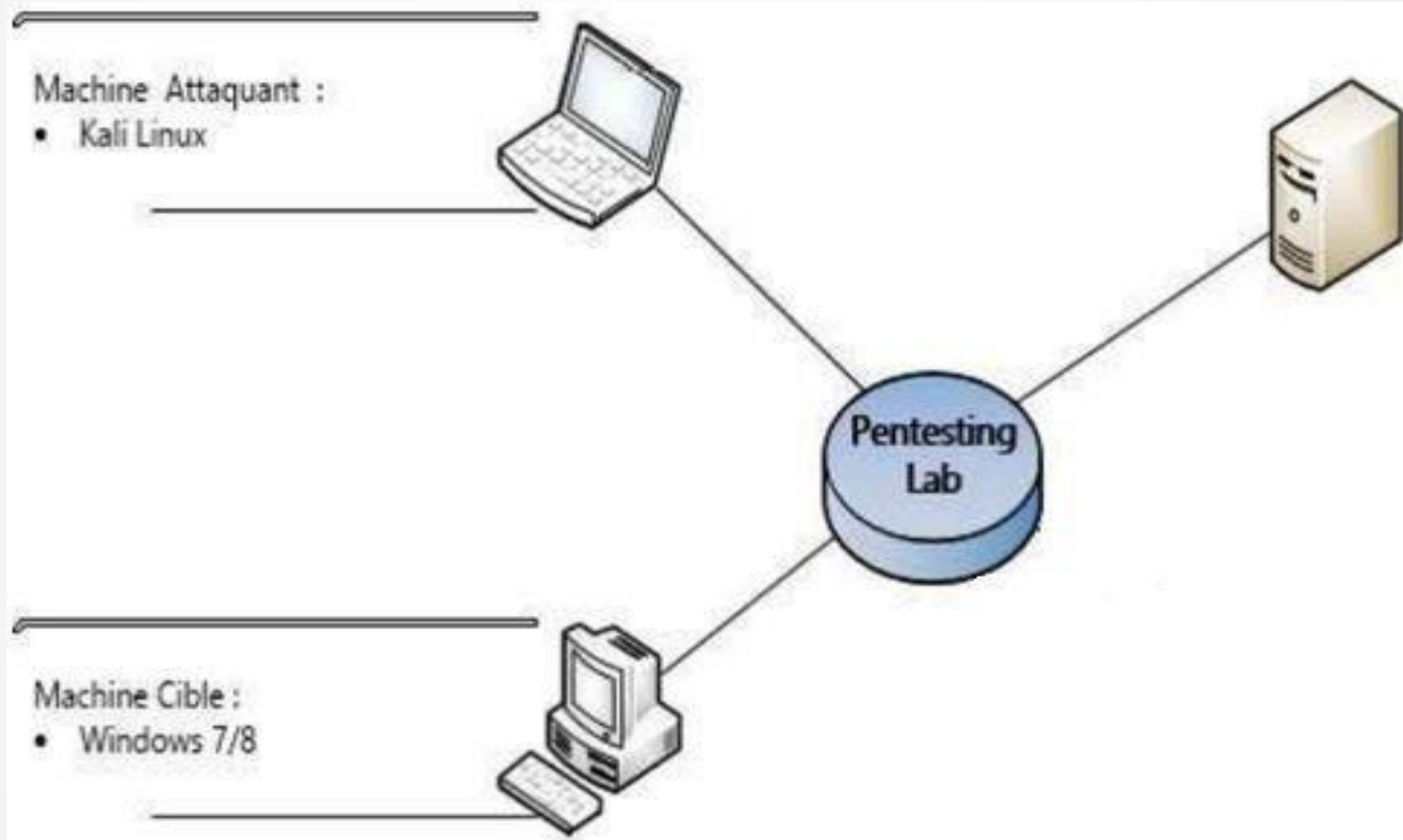


Fin chapitre



Lab : Mise en place de l'environnement de travail

Architecture :



► Lab: Kali Linux



- Kali Linux est une distribution Linux sortie le 13 mars 2013
- Basée sur Debian
- La distribution a pris la succession de Backtrack
- L'objectif de Kali Linux est de fournir une distribution regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information, notamment le test d'intrusion.



► Lab: Metasploitable 2



- La machine virtuelle Metasploitable est une version volontairement vulnérable de Ubuntu Linux conçue pour tester les outils de sécurité et de démontrer les vulnérabilités courantes.
- Cette machine virtuelle est compatible avec VMWare, VirtualBox, et d'autres plates-formes de virtualisation communes.
- Par défaut, les interfaces réseau Metasploitable sont liés au NAT des adaptateurs "réseau local only".

