Université Sidi Mohammed Ben Abdellah
Faculté des Sciences Dhar Mehraz-Fès
Département d'Informatique
Master BDSAS

A.U:2022/2023

Elément de module: Cybersécurité

Par Ismail EL BATTEOUI

Sachez que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'emprisonnement et d'amende.

Avant-propos:

❑ Notion de sécurité:

- La notion de sécurité fait référence à la propriété d'un système, qui s'exprime généralement en termes de:
  - **Disponibilité** (D).
  - I**ntégrité** (I)
  - **Confidentialité** (C).
- Ces critères de base (dits critères DIC) sont des objectifs de sécurité que la mise en œuvre de fonctions de sécurité permet d'atteindre.

Avant-propos:

❑ Notion de sécurité:

- **Disponibilité:**

  La **disponibilité** d'une ressource est relative à la période de temps pendant laquelle le service qu'elle offre est opérationnel.

- **Intégrité:**

  Le critère d'intégrité des ressources est relatif au fait qu'elles sont demeurées intactes, qu'elles n'ont pas été détruites (altération totale) ou modifiées (altération partielle) à l'insu de leurs propriétaires tant de manière intentionnelle qu'accidentelle.

Avant-propos:

❑ Notion de sécurité:

○ **Confidentialité:**

La notion de **confidentialité** est liée au maintien du secret, elle est réalisée par la protection des données contre une divulgation non autorisée .

Il existe deux types d'actions complémentaires permettant d'assurer la confidentialité des données :

- Limiter et contrôler leur accès afin que seules les personnes habilitées à les lire ou à les modifier puissent le faire.
- Les rendre inintelligibles en les chiffrant de telle sorte que les personnes qui ne sont pas autorisées à les déchiffrer ne puissent les utiliser.

Avant-propos:

Notion de sécurité:

Définition:

La sécurité peut être définie en se basant sur les points suivants:

- Assurer qu'un service offert par une ressource pendant une période de temps est opérationnel.
- Les ressources ne doivent subir aucune altération aussi bien partielle que totale.
- Protection des données contre des divulgations non autorisées.

Avant-propos:

❑ Notion de sécurité:

❖ **Domaines d'application:**

La sécurité informatique peut se décliner en :

- Sécurité des systèmes d'information.
- Sécurité des réseaux informatiques.
- Sécurité des conteneurs.
- Etc.

Avant-propos:

❑ Cybersécurité:

- ❖ Actuellement, un grand nombre d'activités sont réalisées *via* **Internet et le cyberespace**.
- ❖ La racine « **cyber** » provient du mot **cybernétique**, qui avait été formé en français en 1834 pour designer la « science du gouvernement ».
- ❖ Terme repris en 1948, par Norman Wiener aux Etats-Unis et qui a donné naissance à la cybernétique, science constituée par l'ensemble des théories relatives au contrôle, à la régulation et à la communication entre l'être vivant et la machine.
- ❖ Depuis lors, le préfixe « cyber » est devenu relatif à l'environnement informatique et aux activités rendues possibles par les technologies du numérique et Internet.
- ❖ La cybersécurité concerne la sécurité informatique et des réseaux des environnements connectés à Internet et accessibles via le **cyberespace**.
- ❖ La cybersécurité peut être mise en défaut, entre autres, par des cyberattaques informatiques.

Plan:

Introduction à la cybersécurité:

Chapitre 1. Vocabulaires et notions de base.

Chapitre 2. Introduction à la sécurité des réseaux informatiques.

Chapitre 3. Introduction à la sécurité des systèmes d'information.

Chapitre 4. Introduction au cryptage des données.

Chapitre1:

Vocabulaires et notions de base

Définition de la cybersécurité:

- La cybersécurité est l'application de technologies, de processus et de contrôles pour protéger les systèmes, les réseaux, les programmes, les dispositifs et les données contre les cyberattaques.
- Elle vise à réduire **le risque** de cyberattaques et à protéger contre l'exploitation non autorisée des systèmes, des réseaux et des technologies.

Types de sécurité:

- **Sécurité des données** : celles contenues au sein d'un système (traitées par la crypto et la théorie des codes).
- **Sécurité des réseaux** : pour les données qui transitent entre des systèmes, dans un environnement distribué ou par un réseau.

Les cinq types de la cybersécurité:

- **Cybersécurité des infrastructures critiques:**
  - Les organisations d'infrastructures critiques sont souvent plus vulnérables aux attaques que les autres car les systèmes reposent souvent sur des logiciels anciens. (les opérateurs de services dans les secteurs de l'énergie, des transports, de la santé, de l'eau,…).
- **La sécurité des réseaux:**
  - Implique le traitement des vulnérabilités affectant les systèmes d'exploitation et l'architecture de votre réseau, notamment les serveurs les hôtes, les pare-feu ,les points d'accès sans fil ainsi que les protocoles de réseau.
- **Sécurité du cloud:**
  - La sécurité du cloud concerne la sécurisation des données, des applications et de l'infrastructure dans le nuage.
- **Sécurité de l'internet des objets:**
  - La sécurité de l'IoT consiste à sécuriser les appareils intelligents et les réseaux connectés à l'IoT.
- **Sécurité des applications:**
  - La sécurité des applications consiste à traiter les vulnérabilités résultant de processus de développement non sécurisés lors de la conception, du codage et de la publication d'un logiciel ou d'un site web.

Risques informatiques:

- Un **risque** se définit comme la probabilité qu'une **menace** exploite une **vulnérabilité** afin d'impacter un **actif.**
- On ne peut pas parler de risque sans que les trois composantes suivantes soient réunies : **vulnérabilité**, **menace**, **coût**.
  - Un **actif** se définit comme tout élément représentant de la valeur pour l'organisation (Un serveur informatique, les application qui y sont installées,…).
  - **Une vulnérabilité est une faille** qui peut être **intrinsèque** à l'actif, c'est-à-dire issue de ses caractéristiques propres, ou **extrinsèque** à l'actif, c'est-à-dire provenant de son environnement externe.
  - Une menace est une vulnérabilité exploitée.
- Test de vulnérabilité:
  - Connaitre les vulnérabilités permet de déterminer la surface d'attaque.
  - Greenbone, OpenVAS,….

Gestion des risques:

- La gestion des risques informatiques est le processus qui consiste à analyser une menace éventuellement présentée par un actif d'une entreprise en évaluant le niveau de risque qu'il est prêt à accepter.
- La gestion du risque ne signifie pas toujours ramener le risque à zéro, mais minimiser le risque lorsque l'impact est important.
- Le processus de gestion des risques informatiques est une tâche qu'une entreprise peut réaliser en interne en utilisant le processus en cinq étapes présenté ci-dessous.
- L'entreprise peut recourir aussi, pour la gestion des risques, à une évaluation externe des risques, telle que la norme ISO 27005.
- Il s'agit d'une norme internationale qui décrit comment réaliser une évaluation des risques en matière de sécurité de l'information.

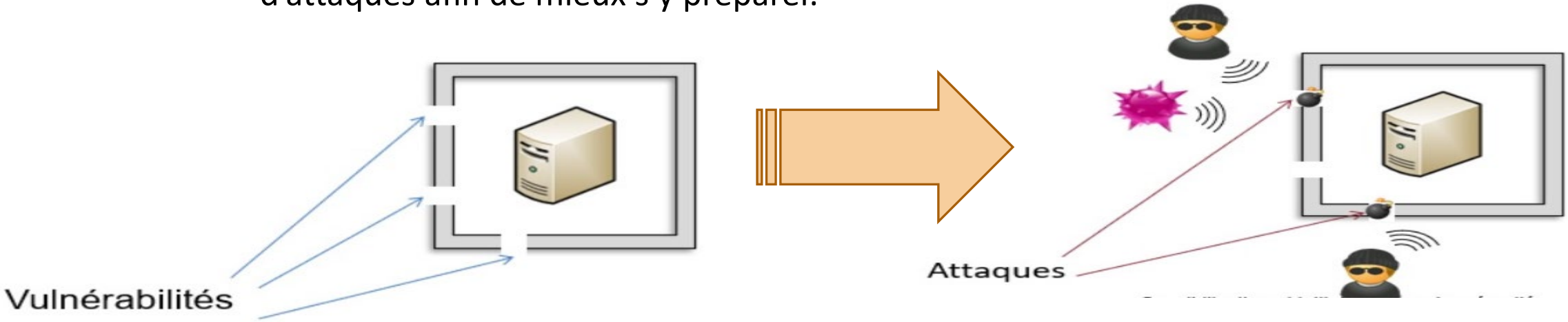
❑ Gestion des risques:

les 5 étapes qu'une entreprise devrait respecter pour identifier les risques informatiques:

- **Identifier les vulnérabilités:** Le service informatique doit définir toutes les faiblesses et tous les risques potentiels liés à l'infrastructure informatique.
- **Identifier et classer les données de l'entreprise:** Il s'agit d'une étape essentielle car une entreprise ne peut protéger les données que si elle sait quelles sont les données à protéger. Cette étape est l'occasion pour l'entreprise d'identifier les données personnelles et sensibles, qui sont les données les plus cruciales à sécuriser et à protéger.
- **Classer les vulnérabilités par ordre de priorité:** Cette tâche doit être effectuée lors d'une réunion conjointe avec le secteur d'activité (LOB en anglais pour Line Of Business), qui peut identifier les systèmes critiques qui doivent être opérationnels en permanence, et le service informatique, qui peut déterminer si les services critiques sont protégés. Au cours de cette étape, le service informatique et le LOB effectueront également :
- **Traiter les risques:** Maintenant que l'entreprise connaît les risques, elle doit les traiter en fonction de la hiérarchisation, de l'appétit au risque et de la tolérance.
- **Effectuer une surveillance continue des risques.**

Attaques informatiques:

- **Définition:** En informatique, une attaque est une tentative d'exposer, de modifier, de désactiver, de détruire, de voler ou d'obtenir un accès non autorisé.
  - **Selon le Comité des systèmes de sécurité nationale des États-Unis d'Amérique (26 Avril 2010):**Toute activité malveillante qui tente de collecter, perturber, nier, dégrader ou détruire les ressources du système d'information ou l'information elle-même.
  - **Une attaque est une 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 avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.
  - Afin de contrer ces attaques, il est indispensable de connaître les principaux types d'attaques afin de mieux s'y préparer.



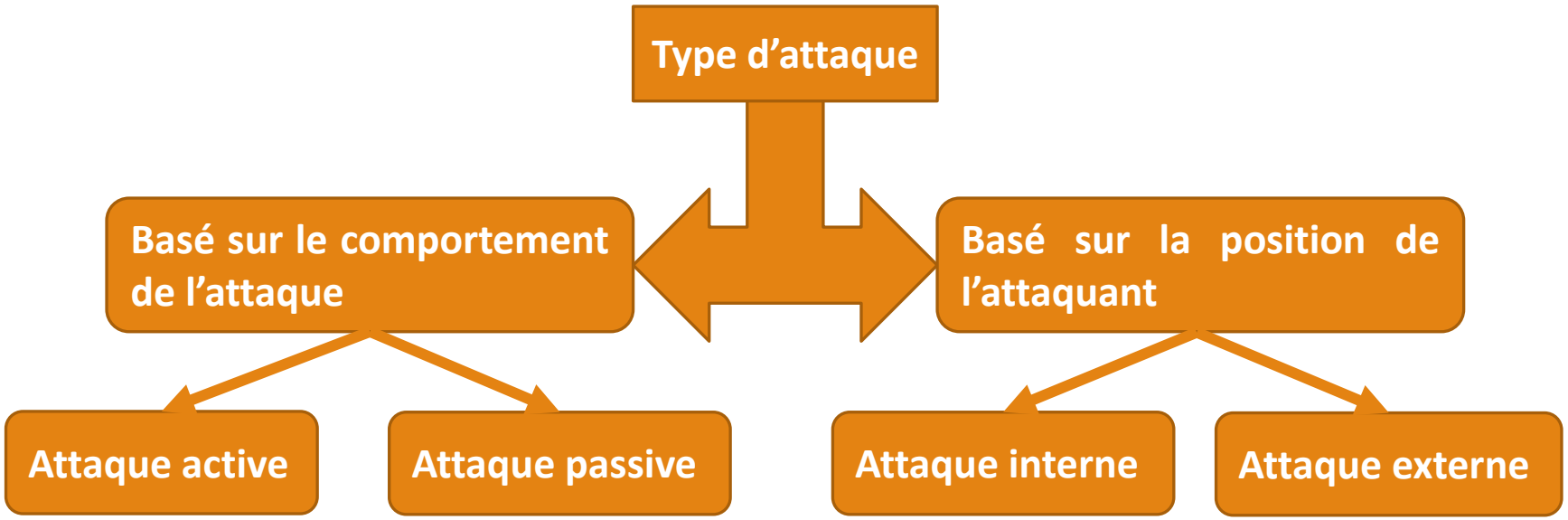
Attaques informatiques:

Objectifs des attaques:

- Obtenir un accès au système.
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles.
- Récupérer des données bancaires.
- S'informer sur l'organisation (entreprise de l'utilisateur, etc.).
- Utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

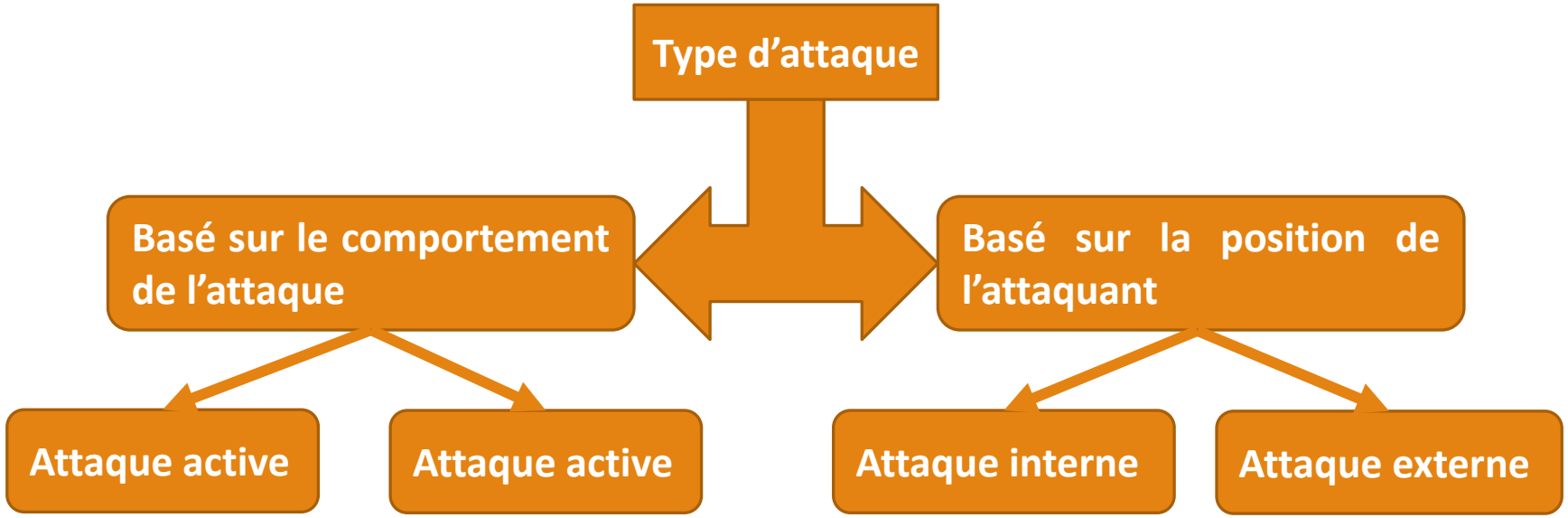
Attaques informatiques:

Types d'attaques:



Attaques informatiques:

Types d'attaques:



- Une **attaque active** tente de modifier les ressources du système ou d'affecter leur fonctionnement.
- Une **attaque passive** tente d'apprendre ou d'utiliser des informations du système mais n'affecte pas les ressources du système.

Chapitre2:

Introduction à la sécurité des réseaux informatiques

❑ Introduction générale:

❖ Rappel sur les réseaux informatiques:

- Voir le TP 2.

❑ Attaques réseaux:

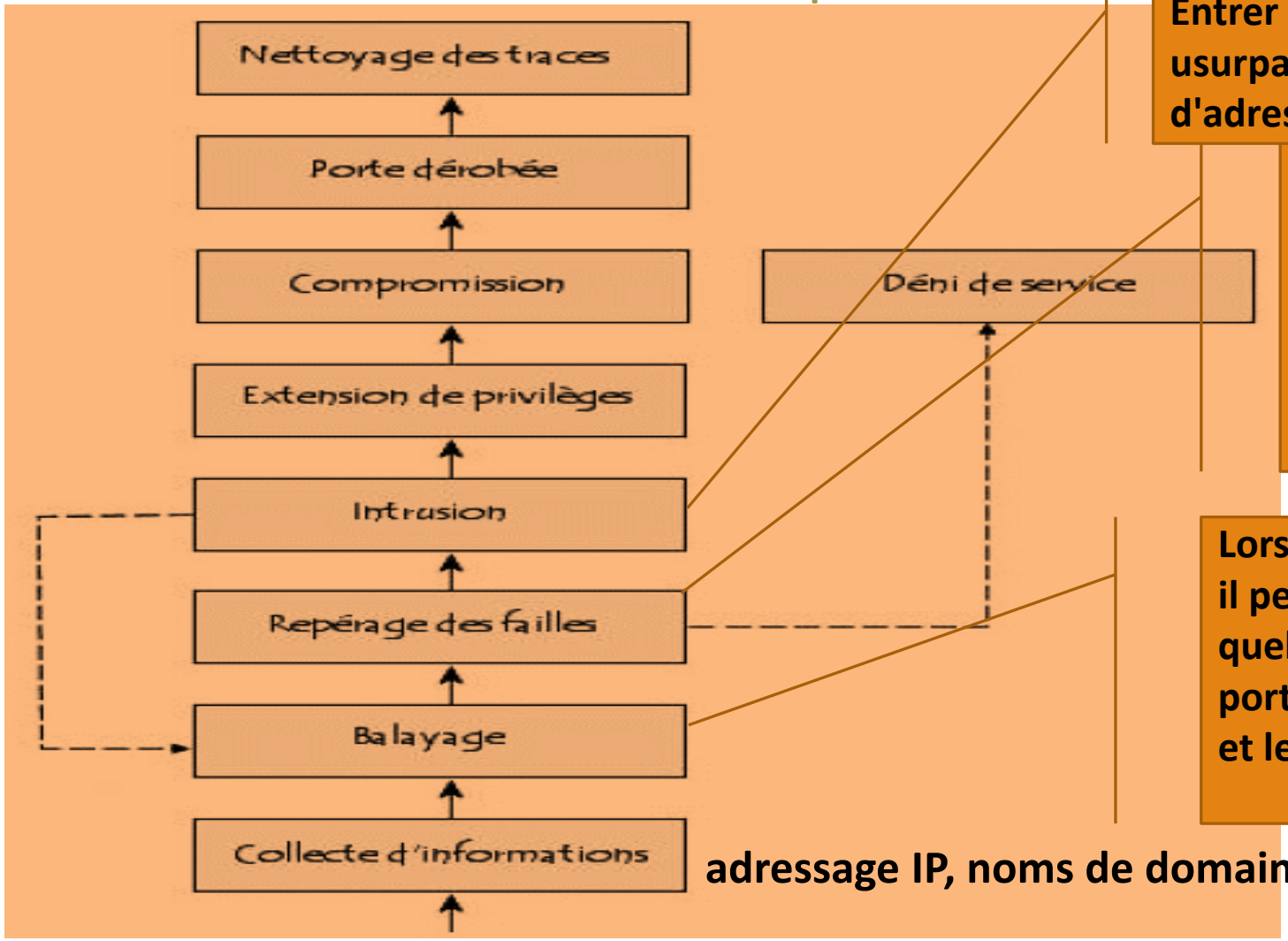
Introduction générale:

- **Rappel sur les réseaux informatiques:**
  - Voir le TP 2.

Scénario d'une attaque réseau:

- La meilleure façon de protéger son système est de procéder de la même manière que les pirates afin d'être en mesure d'identifier les vulnérabilités du système.
- A fin d'exploiter une vulnérabilité, la première étape du hacker consiste à récupérer le maximum d'informations sur les protocoles, sur les systèmes d'exploitation et applications fonctionnant sur celui-ci.
- Le schéma suivant présente le scénario complet:

❑ Scénario d'une attaque réseau:



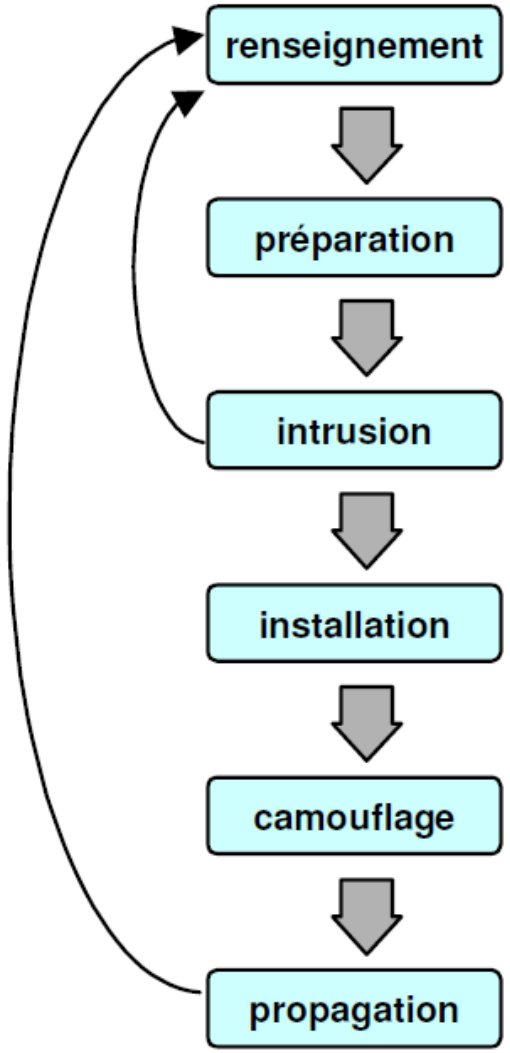
Entrer par un point faible usurpation de nom, d'adresse, cheval de Troie.

Il existe des scanneurs de vulnérabilité permettant aux administrateurs de soumettre leur réseau à des tests d'intrusion afin de constater si certaines applications possèdent des failles de sécurité.

Lorsque la topologie du réseau est connue par le pirate, il peut le scanner:
quelles sont les adresses IP actives sur le réseau, les ports ouverts correspondant à des services accessibles, et le système d'exploitation utilisé par ces serveurs.

adressage IP, noms de domaine, protocoles de réseau, services activés, etc.

Scénario d'une attaque réseau:



découvrir l'architecture du système, son plan d'adressage

dégrader ou contourner la sécurité

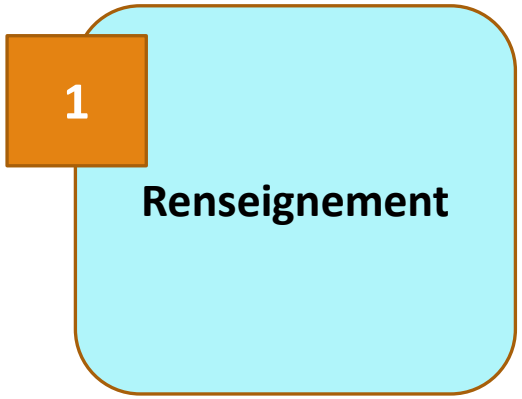
entrer par un point faible

installer une entrée permanente

cacher l'entrée permanente

attaquer les machines ou systèmes en mutuelle confiance

Scénario d'une attaque réseau:



- Le pirate tente d'identifier le plus précisément possible les éléments matériels et logiques participant à l'architecture du système de la victime.
- Les investigations peuvent être mises en œuvre **passivement** au travers de sources ouvertes (sites Internet, presse…) puis complétées a**ctivement** en allant de la simple écoute (Network sniffing: **Wireshark)** d'un réseau à l'espionnage industriel pur et simple, en passant par des techniques de trashing, de détections de services (port scanning) et de détections de systèmes d'exploitation (OS fingerprinting).

❑ Scénario d'une attaque réseau: *Renseignement*

Apprendre à utiliser NMAP

❖ Introduction:

- Nmap (Network Mapper) est un outil open source de scan réseau et d'audit de sécurité.
- Il a été conçu pour rapidement scanner de grands réseaux, mais il fonctionne aussi très bien sur une cible unique.
- Nmap fonctionne en utilisant des paquets IP bruts (raw packets) pour déterminer:
  - Quels sont les hôtes actifs sur le réseau.
  - Quels services (y compris le nom de l'application et la version) ces hôtes offrent.
  - Quels systèmes d'exploitation (et leurs versions) ils utilisent.
  - Quels types de dispositifs de filtrage/pare-feux sont utilisés.
  - Etc.

❑ Scénario d'une attaque réseau: *Renseignement*

Apprendre à utiliser NMAP

❖ Introduction:

- Le rapport de sortie de Nmap est une liste des cibles scannées ainsi que des informations complémentaires en fonction des options utilisées.
- L'information centrale de la sortie est la « table des ports intéressants ». Cette table liste le numéro de port et le protocole, le nom du service et son état.
- L'état est soit `ouvert (open)`, `filtré (filtered)`, `fermé (closed)` ou `non-filtré (unfiltered)`.
- `Ouvert` indique que l'application de la machine cible est en écoute de paquets/connexions sur ce port.
- `Filtré` indique qu'un pare-feu, un dispositif de filtrage ou un autre obstacle réseau bloque ce port, empêchant ainsi Nmap de déterminer s'il s'agit d'un port `ouvert` ou `fermé`.
- Les ports `fermés` n'ont pas d'application en écoute, bien qu'ils puissent quand même s'ouvrir n'importe quand.

https://nmap.org/

Scénario d'une attaque réseau: *Renseignement*

Apprendre à utiliser NMAP

Introduction:

- En plus de la table des ports intéressants, Nmap peut aussi fournir de plus amples informations sur:
  - les cibles comme les noms DNS (reverse DNS).
  - Deviner les systèmes d'exploitation utilisés.
  - Obtenir le type de matériel ou les adresses MAC.

Scénario d'une attaque réseau: *Renseignement*

Apprendre à utiliser NMAP

- Syntaxe:

```
nmap [Type(s) de scan] [Options] {spécifications des cibles}
```

SPÉCIFICATIONS DES CIBLES:

Les cibles peuvent être spécifiées par des noms d'hôtes, des adresses IP, des adresses de réseaux, etc.

Exemple:

```
# Scanning a specific hostname:
nmap hostname
# Scanning a specific IP address:
nmap @ip
# Scanning a network range:
nmap X.Y.Z.1-254 or nmap X.Y.Z.0/24
# Scanning a network range but exclude few IP addresses:
nmap X.Y.Z.0/24 --exclude X.Y.Z.167
```

❑ Scénario d'une attaque réseau: *Renseignement*

Apprendre à utiliser NMAP

❖ Syntaxe:

```
nmap [Type(s) de scan] [Options] {spécifications des cibles}
```

Options:

Nmap propose des centaines d'options. Voici les plus utilisées:

•Sauvegarde : Pour sauvegarder vos scan dans un fichier, utilisez l'option -oN

•Verbosity : Pour rendre Nmap plus bavard à l'écran -v, -vv, -vvv

•Timing : Vous pouvez utiliser des *timing template* en utilisant l'un des flags -T0,-T1,-T2,-T3,-T4,-T5

Types de scan Nmap courants

•Scan SYN (-sS) identifie un port qui doit être ouvert en envoyant un "SYN" à la cible. Si elle reçoit un SYN-ACK ou un SYN, elle marque ce port comme étant ouvert. S'il reçoit un "RST", il marque le port comme étant filtré (filtered), c'est à dire inaccessible à cause d'un pare-feu par exemple.

•Scan TCP (-sT) identifie un port comme étant ouvert en attendant la fin du *three-way handshake*.

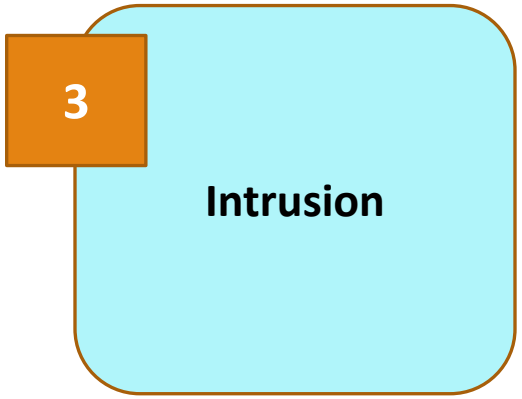
•Scan UDP (-sU) est utile pour identifier les ports UDP ouverts sur une cible. Il envoie des paquets UDP spécifiques à des ports UDP connus.

❑ Scénario d'une attaque réseau: *Renseignement*

Apprendre à utiliser NMAP

- ❖ Travaux pratiques

❑ Scénario d'une attaque réseau:



Recherche de vulnérabilités par Metasploit:

- L'intrusion est le fait pour une personne ou un objet de pénétrer, dans un espace (physique, logique ou relationnel) défini où sa présence n'est pas souhaitée. La notion d'intrusion suppose qu'il existe une volonté de réserver l'accès à des personnes, des ressources physiques ou logiques, à certaines personnes désignées. (Wikipédia)
- Test d'intrusion peut être réalisé afin de détecter les vulnérabilités informatiques d'un système.
- Pour détecter les vulnérabilités, plusieurs approches peuvent être adoptées. Dans ce cours on utilisera le Framework Metasploit.

❑ Scénario d'une attaque réseau: Intrusion (Test)

Apprendre à rechercher des vulnérabilités par Metasploit:

❖ Définition:

Metasploit est un framework fournissant une infrastructure permettant l'automatisation de tâches de test d'intrusion. Il permet d'identifier, d'exploiter etc... des failles de sécurité dans des programmes, systèmes d'exploitation application lourde et application web etc...

❖ Architecture de Metasploit:

exploit : Un exploit est un code d'exploitation par lequel un attaquant pourra profiter d'un défaut système afin de s'introduire ou de réaliser des action non prévues sur ce système.

❑ Scénario d'une attaque réseau: Intrusion (Test)

Apprendre à rechercher des vulnérabilités par Metasploit:

❖ Architecture de Metasploit:

Auxiliary : Les modules auxiliary sont souvent des outils de scan tel que les scans de port ouvert d'une machine cible ou de services.

Posts : Les modules posts ou module de post-exploitation sont des modules permettant d'accéder aux données confidentielles tel que des identifiants ou des mots de passes de services ou d'applications. Ces modules sont utilisés une fois une cible compromise afin d'élargir notre surface d'attaque ou de gagner des accès.

Payload : Un payload est un code qu'un attaquant souhaitera exécuté à distance sur une machine cible comme par exemple un reverse shell qui permet d'ouvrir une connexion depuis la machine cible vers la machine attaquante.

❑ Scénario d'une attaque réseau: Intrusion (Test)

Apprendre à rechercher des vulnérabilités par Metasploit:

- ❖ Recherche de vulnérabilités:
  - ➢ Scan de réseau avec Metasploit: Voir le travail pratique
  - ➢ Recherche de vulnérabilités :Voir le travail pratique