UNIVERSITE BATNA 2
FACULTE MATHEMATIQUES&INFORMATIQUE
DEPARTEMENT INFORMATIQUE
LICENCE 3 ISIL
Module Sécurité Informatique

CHAPITRE 3 : Attaques et Mécanismes de défense

Aspects de la sécurité informatique

1- Sécurité physique :

- Aspects liés au matériel (Routeurs , Serveurs, Postes clients, Équipements mobiles…)
- Aspects liés à l'environnement : locaux, alimentation électrique, climatisation,…

Mesures :

- ✓qualité du bâtiment;
- ✓contrôles des accès;
- ✓redondance physique;
- ✓redondance dans les technologies de communication utilisées ;
- ✓qualité de l'alimentation électrique .

Aspects de la sécurité informatique

2- Sécurité logique :

- Aspects liés à la protection du système d'exploitation, ….

Mesures :

- ✓ Contrôle d'accès logique : identification, authentification, autorisation, séparation des privilèges;
- ✓ Protection des données : cryptage, anti-virus, sauvegarde.

Aspects de la sécurité informatique

4- Sécurité du réseau et des télécommunications :

- nécessité d'une infrastructure réseau sécurisée

Mesures :

- ✓contrôle d'accès aux services offerts via le réseau
  - ✓Au niveau des accès
  - ✓Au niveau des protocoles
  - ✓Au niveau des équipements
- ✓authentification du correspondant et de l'origine des données

Mécanismes de défense

Que couvre la sécurité en général ?

Prévention

- ✓ Prendre des mesures afin d'empêcher les biens et les actifs d'être attaqués.

Détection

- ✓ Prendre des mesures afin de détecter quand, comment, par qui un actif ou un bien a été endommagé.

Réaction

- ✓ Prendre des mesures après un incident de sécurité afin de pouvoir restaurer les biens et les actifs, ou réduire l'impact de l'incident.

- il existe de nombreux moyens techniques permettant d'assurer la protection d'un système informatique :
  - la cryptographie
  - la restriction d'accès par mot de passe
  - les antivirus
  - les pare-feux
  - les systèmes de détection d'intrusions
  - les renifleurs de paquets
  - Etc.

Mécanismes de défense

- *Protection physique*

- *Cryptage (chiffrement)*
  - Utilisation d'algorithmes mathématiques pour transformer les messages en une forme inintelligible (**confidentialité**).

- *Signature numérique*
  - Ajout de données à une unité de données afin de prouver la source (**authentification**) et **l'intégrité** de cette unité de données.

- *Authentification*
  - Mécanisme assurant l'identité d'une entité à travers un échange d'information : mot de passe, carte à puce, biométrie (empreinte digitale, oculaire ou vocale)…

Mécanismes de défense

- *Antivirus*
  - Une application censée protéger la machine contre des codes néfastes (malveillants).
- *Pare-feu (Firewall)*
  - Logiciel ou matériel informatique qui contrôle la politique de sécurité et les accès autorisés ou pas au sein du réseau.
  - Protège des attaques externes.
- *Système de Détection d'Intrusions (IDS)*
  - Repère et détecte les activités suspectes sur le réseau et les signale à l'administrateur .

Mécanismes de défense

- *Notarisation*
  - La notarisation électronique permet la vérification et l'archivage des preuves d'échanges et d'archivage électroniques par un tiers de confiance agréé (à la manière d'un notaire).

- *Horodatage (Timestamping)*
  - Mécanisme qui consiste à associer une date et un temps correct à un événement, une information ou une donnée informatique pour enregistrer l'instant auquel une opération a été effectuée. Sert surtout pour la **Non-répudiation.**

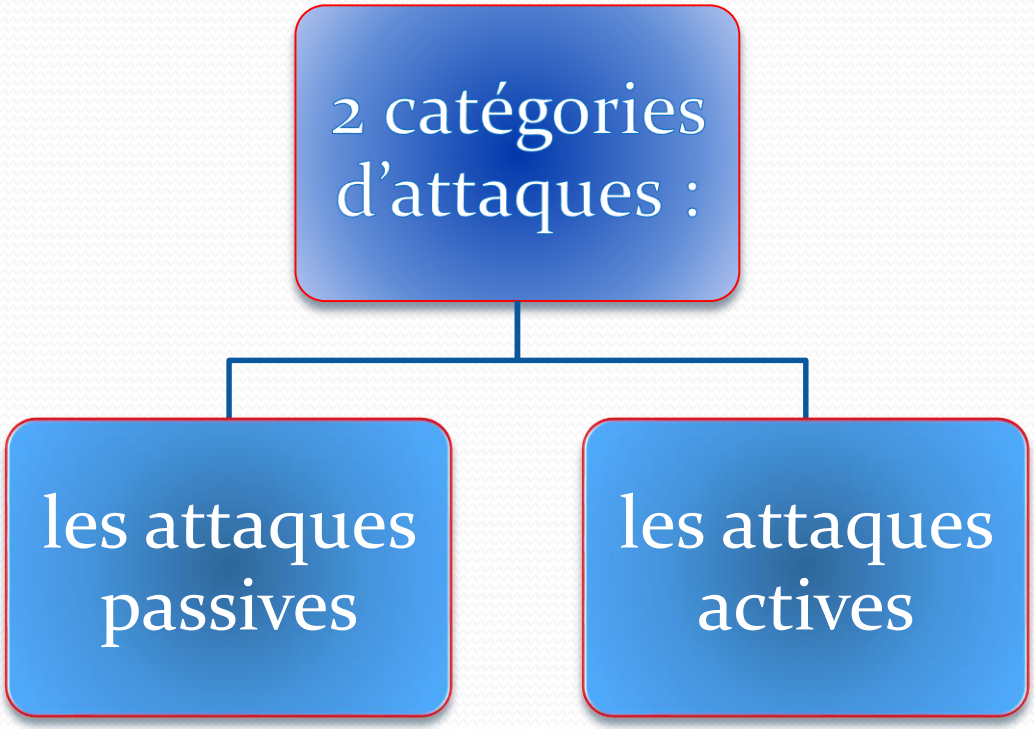
- *Bourrage de trafic (Traffic Padding)*
  - Insertion d'un certain nombre de bits supplémentaires au niveau d'un flux de données pour faire échouer les tentatives d'analyse du trafic et assurer la **confidentialité.**

Mécanismes de défense

- *Contrôle d'accès*
  - Vérifier si une entité (une personne, une machine …) demandant d'accéder à une ressource a les **droits nécessaires** pour le faire.
- *Certification*
  - Certificat électronique ou numérique: carte d'identité numérique, utilisé pour **identifier et authentifier** une personne physique ou morale.
- *VPN (Virtual Private Network) et tunnels*
  - Mécanisme qui consiste à relier deux réseaux ou sous-réseaux par un tunnel sécurisé.

Attaques

Attaque : action malveillante qui tente d'exploiter une faiblesse dans le système et de violer un ou plusieurs besoins de sécurité.


2 catégories d'attaques :
les attaques passives
les attaques actives

Attaques passives et attaques actives

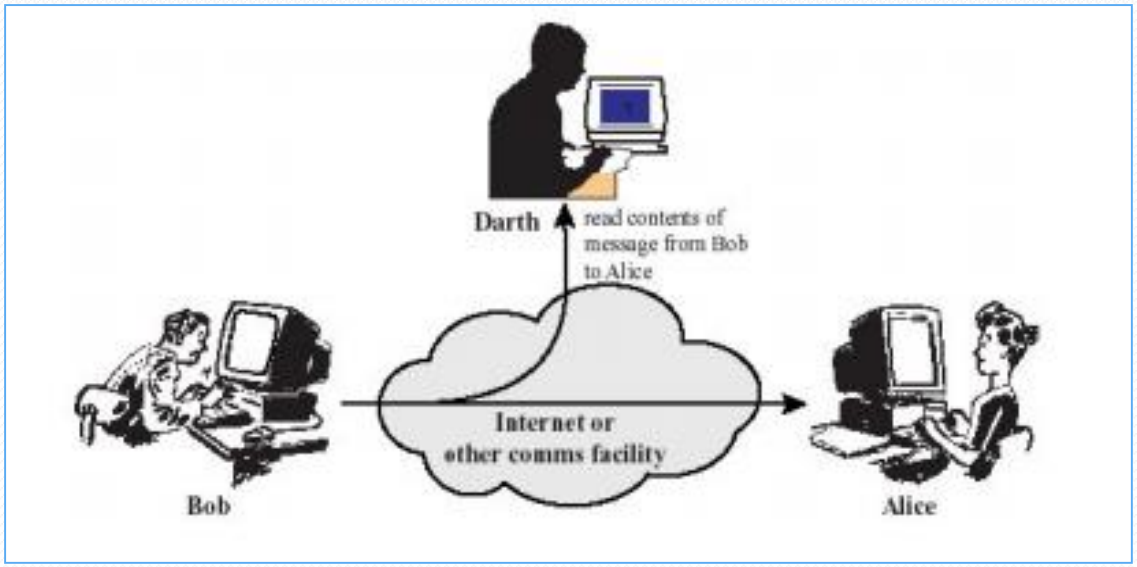
Attaques passives :

- ✓ collecter ou utiliser des informations relatives au système de manière illicite
- ✓ n'affectent pas les ressources du système

Attaques actives :

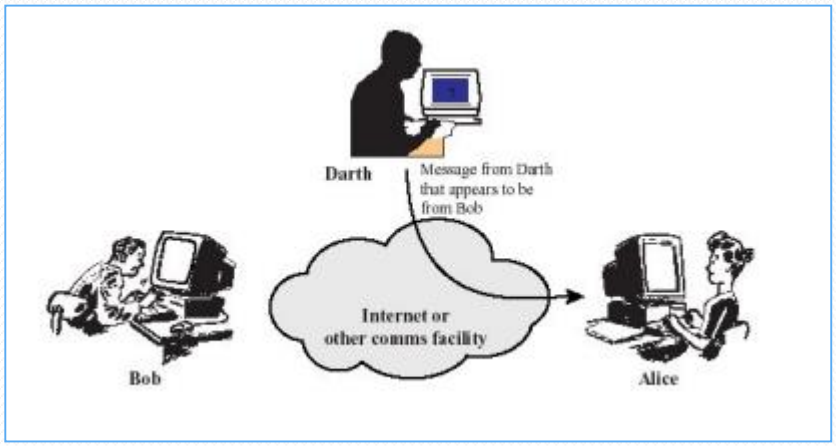
- ✓ altérer des informations
- ✓ affecter le bon fonctionnement d'un service

Interception / Analyse de trafic

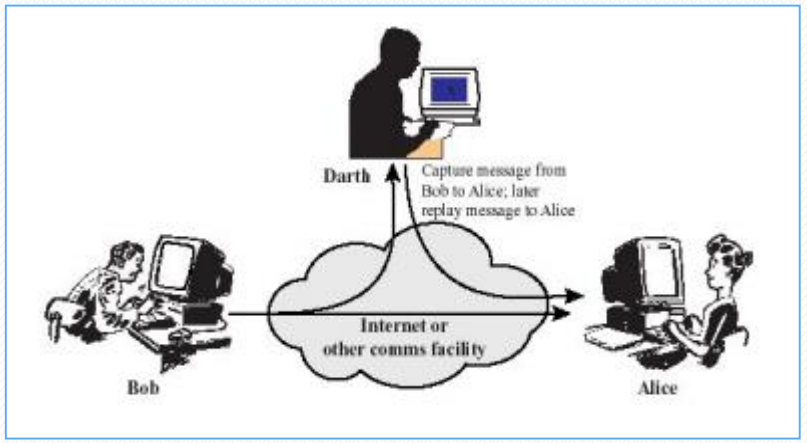


Attaques actives

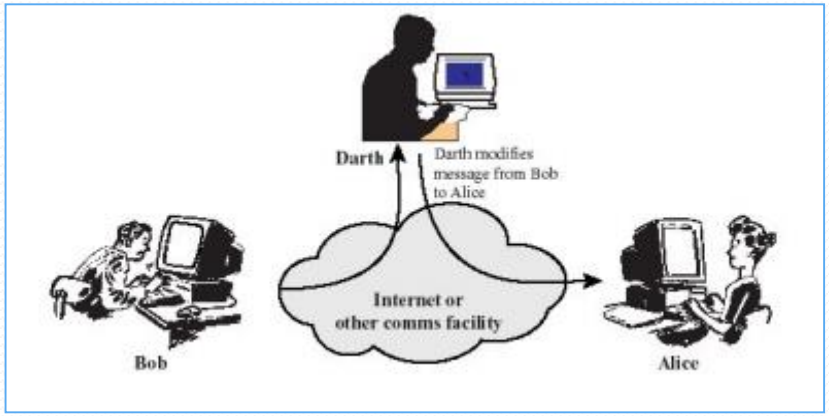
Mascarade



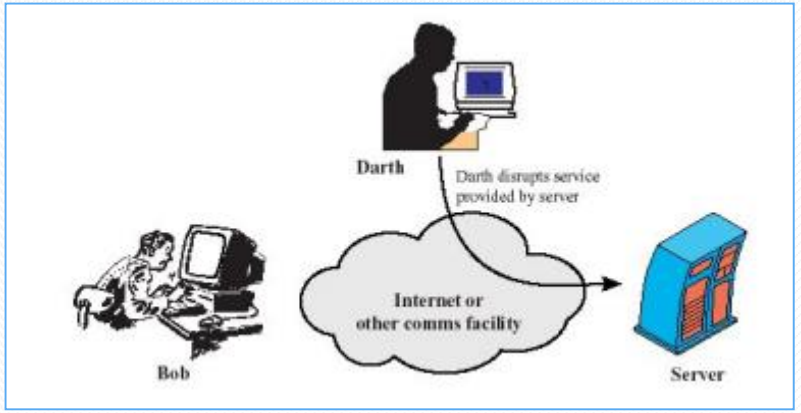
Rejeu



Man in the middle



DoS



Programmes malveillants

✓ logiciel développé dans le but de nuire à un système informatique.

❑ **Les virus**

- But : consommer ou paralyser des ressources système
- Besoin d'un programme hôte
- S'auto-duplique pour mieux infecter le système
- Transmission : courrier électronique , échange de données
- Effets d'une contamination : fichiers effacés, disque dur formaté, saturation des disques, modification du MBR, etc.

Programmes malveillants

- **Les vers (worms)**
  - Programme autonome et indépendant
  - Transmission : réseau
- **Les bombes logiques**
  - une partie d'un programme malveillant (virus, cheval de Troie, etc.)
  - besoin d'un détonateur pour s'activer
- **Les chevaux de Troie (trojan)**
  - Programme à apparence légitime qui exécute des routines nuisibles sans l'autorisation de l'utilisateur

Programmes malveillants

- **Les portes dérobées (backdoors)**
  - Logiciel de communication caché
  - Accès cachés (accès réseau frauduleux)

- **Le rootkit**
  - Ensemble de logiciels et de fichiers cachés dans l'OS, permettant :
    - obtenir les droits d'administrateur sur une machine,
    - installer une porte dérobée,
    - truquer les informations susceptibles de révéler la compromission,
    - effacer les traces laissées par l'opération dans les journaux système

Attaques liées à la messagerie électronique

- **Les pourriels (spams)**
  - courrier électronique d'exemplaires identiques,
    - envoyé en nombre
    - de façon automatique et non-sollicité (but publicitaire ou promotionnel)
  - encombrent le réseau,
  - font perdre du temps à leurs destinataires.

- **L'hameçonnage (phishing)**
  - courrier électronique dont l'expéditeur se fait généralement passer pour un organisme financier (site de commerce électronique, banque…),
  - demande au destinataire de fournir des informations confidentielles.

Attaques liées à la messagerie électronique

- **Le canular informatique (hoax)**
  - fausse information ou rumeur,
  - courrier électronique incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes,
  - incitent l'utilisateur à effectuer des manipulations dangereuses sur son poste,
  - encombrent le réseau,
  - font perdre du temps à leurs destinataires.

Attaques contre les firewalls

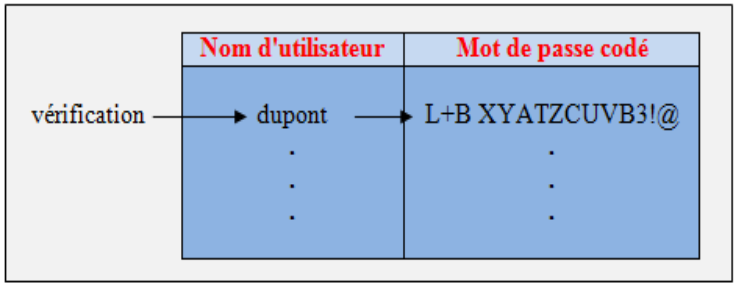
- **Scanner de port**
  - Nmap (Network Mapper), Firewalk et Hping2
  - Nmap , scanner de port le plus célèbre disponible sous linux, Windows et même MAC

- **Comment s'en protéger ?**
  - Configurer votre pare-feu pour empêcher les scans

Craquage de mots de passe

connexion utilisateur au système d'information:

- **nom d'utilisateur** (username)
- **mot de passe** (password)
  - encryptés pour garantir leur confidentialité
  - stockés dans des listes de mots de passe sur des fichiers systèmes prédéfinis



Problème de base : faire en sorte que les mots de passe ne puissent pas être facilement devinés.

Craquage de mots de passe

perceur de mot de passe

- **L'attaque par dictionnaire**
- **Le brute forcing**

Différents logiciels de perçage de mots de passe en fonction du type d'encryptage (DES, MD5, special Microsoft …)

- **Comment s'en protéger ?**
  - Choisir le bon mot de passe
  - Emploi d'une carte ou d'un badge
  - Emploi des caractéristiques de l'utilisateur
  - …

Attaques réseau

- **Les écoutes (*sniffing*)**
  - Technique permettant de récupérer toutes les informations transitant sur un réseau,

  - **Comment s'en protéger ?**

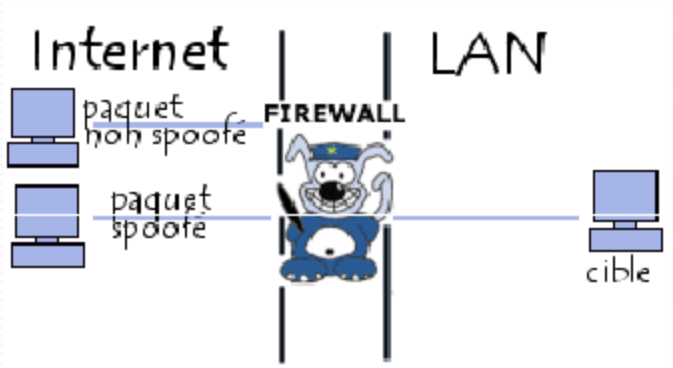
Difficile: un sniffer est passif, il n'envoie aucun paquet, il ne fait qu'intercepter

- carte réseau : son temps et sa façon de répondre à certains paquets sont modifiés

  ➔ présence d'un sniffer
- "tunneler" toutes les transactions (VPN, IpvSec…)
- cryptographie

Attaques réseau

- **L'usurpation d'identité (spoofing)**
  - prendre l'identité d'une autre personne ou d'une autre machine

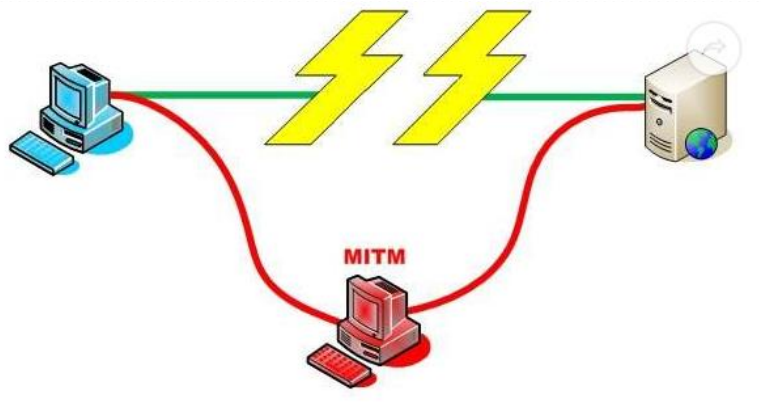


  - L'IP spoofing se base sur une usurpation d'adresse IP

- **Comment s'en protéger ?**
  - supprimer tous les services se basant sur l'authentification IP (rlogin, rsh)
  - "tunneler" toutes les transactions (VPN, …)

Attaques réseau

- **Homme-au-milieu(Man-in-the-Middle)**
  - Technique de piratage informatique consistant à intercepter des échanges cryptés (méthode d'échange de clés par exemple)entre deux personnes ou deux ordinateurs pour décoder les messages
  - Pour écouter, altérer ou détruire les informations transmises, ou prendre le contrôle d'un serveur
  - Une attaque connue dans cette catégorie repose sur une compromission des tables ARP (ARP Poisoning).



Attaques réseau

- **Le déni de service (Denial Of Service)**
  - Il s'agit de saturer un réseau ou un système pour le rendre inopérant
    - Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise,
    - Peut être provoquée par une seule machine (DoS) ou simultanément par plusieurs machines (Distributed DoS).
  - De très nombreuses méthodes permettent d'arriver à un DoS :
    - **le SYN flood** consiste à saturer un serveur en envoyant un grand nombre de paquets TCP avec le flag SYN ,
    - **l'UDP flood** consiste à saturer le trafic réseau en envoyant un grand nombre de paquets UDP à une machine,
    - **les bombes e-mail** consistent à envoyer sur le réseau des mails trop volumineux
    - Etc…