Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Centre Universitaire de Mila
Institut des Sciences et de la Technologie

Administration des Réseaux

– Chapitre 4 – Sécurité des Réseaux:

Partie 1: Concepts de la sécurité informatique

Département MI

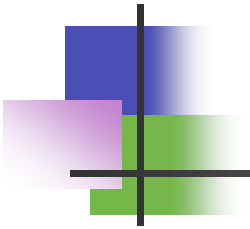
Objectifs

Objectif du cours

✓Maîtriser les notions de base relatives à la sécurité

✓Connaitre les objectifs de la sécurité et les mécanismes à mettre en place pour assurer la sécurité des systèmes d'information

✓Connaitre les notions de base relatives à l'audit informatique

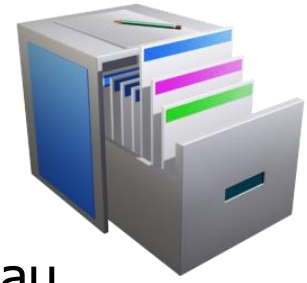


Securité des systèmes informations

Plan

- Definitions
- Objectifs de la sécurité informatique
- Sources de vulnérabilité des systèmes informatiques
- Types des menaces
- Origines et types des attaques
- Les effets d'une attaque
- Principaux outils de défense
- Politique de sécurité

Définitions (1/3)



système d'information :

→ L'ensemble des **moyens** nécessaires à l'élaboration, au traitement, au stockage, à l'acheminement et à l'exploitation des **informations**

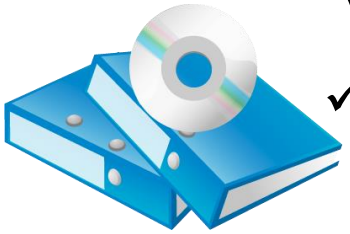
→SI représente un **patrimoine** essentiel de l'entreprise

→la **confidentialité** et la **disponibilité** de l'information constitue un enjeu très important pour la compétitivité de l'entreprise

Définitions (2/3)

La sécurité du système d'information :

→ Ensemble de **mesures** de sécurité **physique**, **logique**, administrative et de mesures d'urgence, mises en place dans une organisation, en vue d'assurer:



✓La confidentialité des **données** de son système d'information

✓ La protection de **ses biens** informatiques

✓La continuité de **service**

Définitions (3/3)

→Les systèmes informatiques sont **au cœur** des systèmes d´information

→Ils sont devenus la cible de ceux qui **convoitent** l'information

→ Assurer la sécurité de l'information **implique** l'assurance de la sécurité des systèmes informatiques.

La sécurité informatique

La science qui permet de s'assurer que celui qui **consulte** ou **modifie** des **données** du système en a l'**autorisation**

Objectifs de la sécurité informatique

Les principaux objectifs à garantir:

Authentification : vérifier l'**identité** des personnes qui veulent **manipuler** l'information

Confidentialité : L'information ne peut être connue que par les personnes autorisées

Disponibilité : L'information doit être **utilisable** à la demande

Intégrité : L'information ne doit pas être **altérée** ou **détruite** par accident ou malveillance

Non répudiation : L'absence de possibilité de **contestation** d'une action une fois celle-ci est effectuée

Pourquoi les systèmes sont-ils vulnérables ?(1/2)

Vulnérabilité

→**Faille** ou **bug** pouvant être utilisé pour obtenir un niveau d'accès **illicite** à une ressource d'informations ou des privilèges supérieurs à ceux considérés comme normaux pour cette ressource

→La vulnérabilité caractérise les composants du système(matériel, logiciel, les règles, les procédures, personnel) **susceptibles** d'être attaquées avec succès

→Une vulnérabilité est exploitée par **une menace pour causer** une perte

→Exemples de **vulnérabilités :**
✓ Utilisation des **mots de passe** non **robustes**
✓Présence de comptes **non protégés** par mot de passe

Pourquoi les systèmes sont-ils vulnérables ?(2/2)

✓La sécurité est ***cher*** et ***difficile***: Les organisations n'ont pas de **budget** pour ça

✓La sécurité ne peut être sûr à **100%**, elle est même souvent **inefficace**

✓La politique de sécurité est **complexe** et basée sur des jugements humains

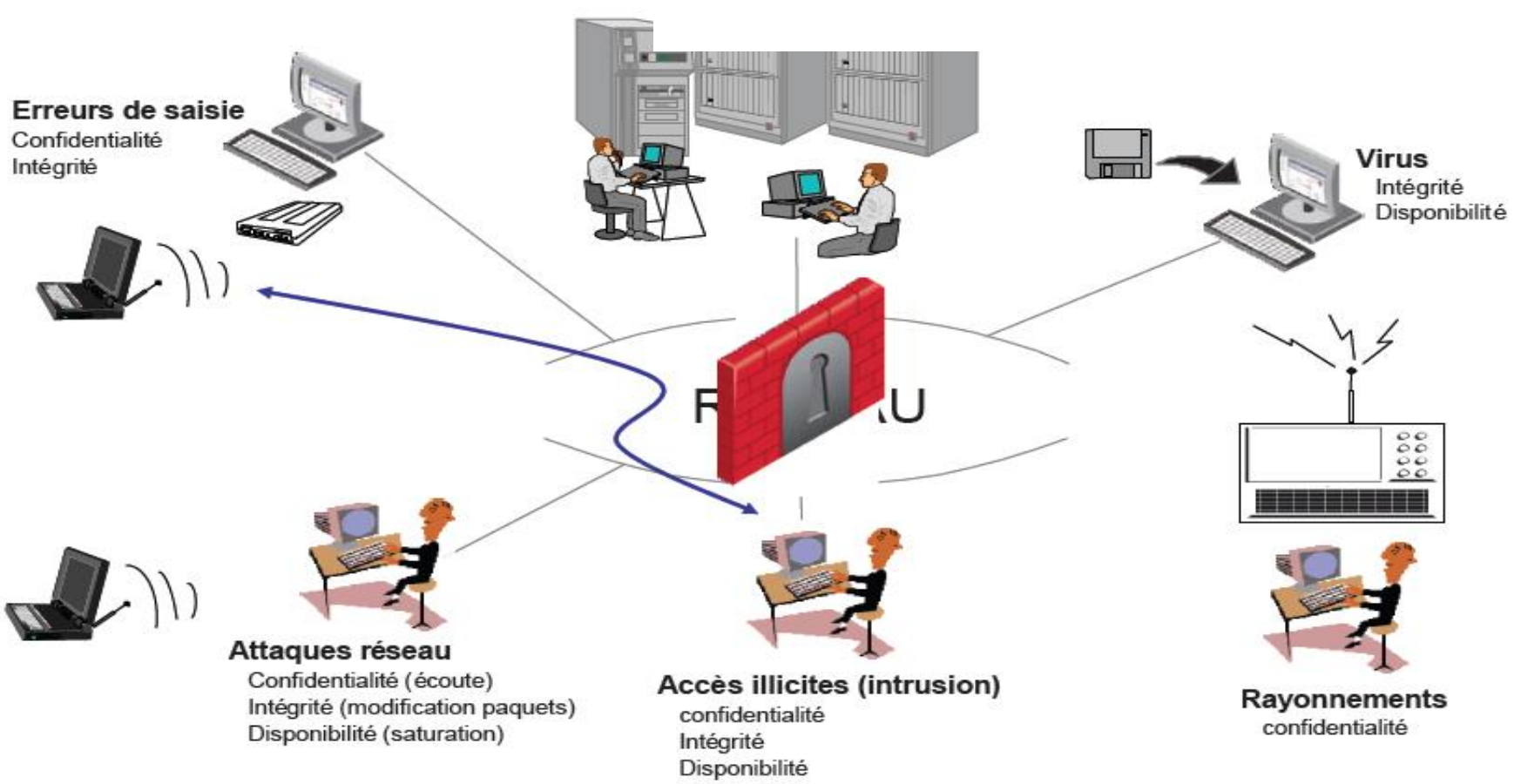
✓Les organisations acceptent les **risques**, la sécurité n'est pas une priorité

✓De nouvelles technologies (et donc vulnérabilités) **émergent** en permanence

✓Les systèmes de sécurité sont faits, gérés et configurés par des **hommes**

✓ …

Les types des menaces(1/2)

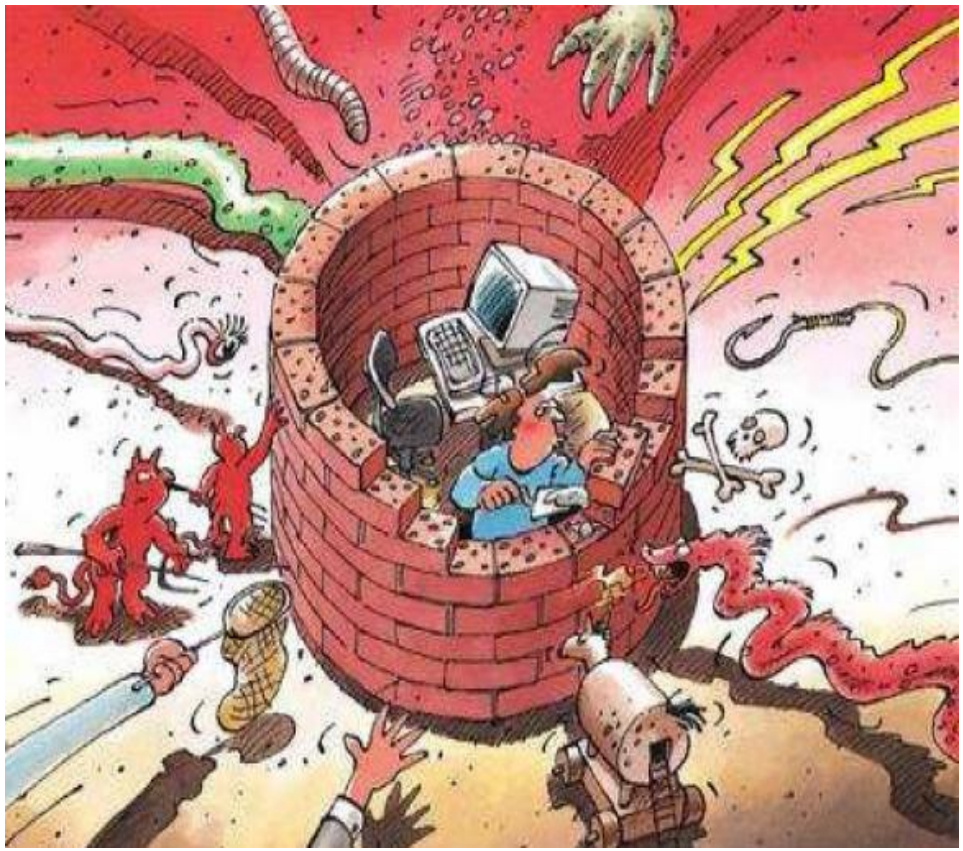


Les types des menaces(2/2)

accidentelle

- ✓ **Panne disque**
- ✓ **Chute de tension**
- ✓ **Echange des disquettes infectée**

…



intentionnels

- ✓ **Le vol**
- ✓ **L'écoute**
- ✓ **La fouille**

…

Les Types d'attaques(1/5)

Les attaques d'accès

Les attaques de modification

Les attaques par saturation (déni de service)

Les attaques de répudiation

Attaque = cible + méthode + Vulnérabilités

Les Types d'attaques(2/5)

Les attaques d'accès

✓ Ingénierie **sociale** ou Système D : L'attaquant établit des relations avec le **personnel** et **piéger** les gens pour obtenir des informations sur les **mots de passe**, La **topologie du réseau**,…

✓ Portes **dérobées** (backdoors) : injecter un **code** dans la cible pour l'**exploiter** plus tard

✓ **Sniffing** : L'attaquant se met à l'**écoute** sur le réseau pour obtenir des informations

✓…

Les Types d'attaques(3/5)

Les attaques de modification

✓**Virus**: un programme caché dans un autre qui peut s'exécuter et se reproduire en infectant d'autres programmes ou d'autres ordinateurs

✓**Ver**: un programme qui se *copie lui-même* mais qui n'affecte pas d'autres fichiers → relâcher un ver dans internet permet de ralentir le trafic

✓**Bombe logique**: un programme qui se déclenche à une **date** ou à un **instant donnée**

✓**Macro virus**: Ils sont insérés dans certains fichiers d'extensions doc, xls, ppt…et ils donnent la possibilité d'exécuter de petits programmes spécifiques sur le document qui les contient

✓**Cheval de Troie**: est un programme qui lui est un ver ou autre type de programme aux effets pervers

Les Types d'attaques(4/5)

Les attaques par saturation (déni de service)

✓**Flooding**: Envoyer à une machine de nombreux paquets **IP** de grosse taille**.** La machine cible ne pourra pas traiter tous les paquets et finira par se **déconnecter** du réseau**.**

✓**Ping de la mort** (Ping Of Death): Envoyer un paquet **1** octet plus gros que le datagramme du **ping.** Fragmentation du ping et à l'arrivée le serveur se bloque en tentant de **recoller** les fragments**.**

✓**Smurf**: S'appuie sur le ping et les serveurs de broadcast**.** On falsifie d'abord son adresse **IP** pour se faire passer pour la machine cible

✓**Débordement de tampon**: On envoie à la machine cible des données d'une **taille supérieure** à la capacité d'un paquet**.** Celui-ci sera alors **fractionné** pour l'envoi et rassemblé par la machine cible→ il y aura débordement des **variables internes**.

Les Types d'attaques(5/5)

Les attaques de répudiation

✓Le **IP spoofing**: se faire passer pour une autre machine en falsifiant son adresse IP (Elle est en fait assez complexe)

Les effets d'une attaque

Attaque passive : c'est la moins dangereuse

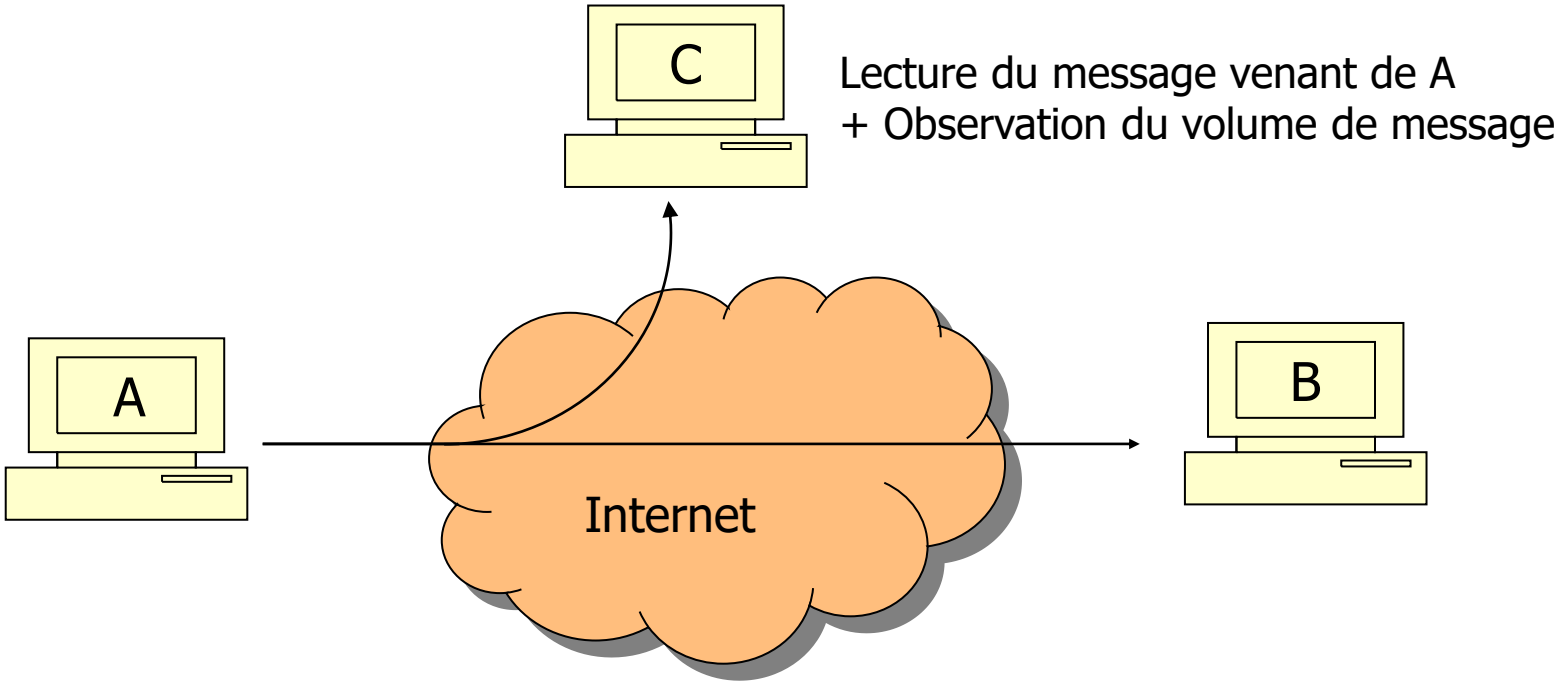
- Ne **modifie** pas l'information
- **Consultation** de l'information

Attaque active : ce type d'attaque est dangereux

- **Modifie** l'état d'une information, d'un serveur ou d'une communication
- Connexion frauduleuse à un host ou un réseau
- **Altération** des messages en transit sur un réseau (Denis de service)

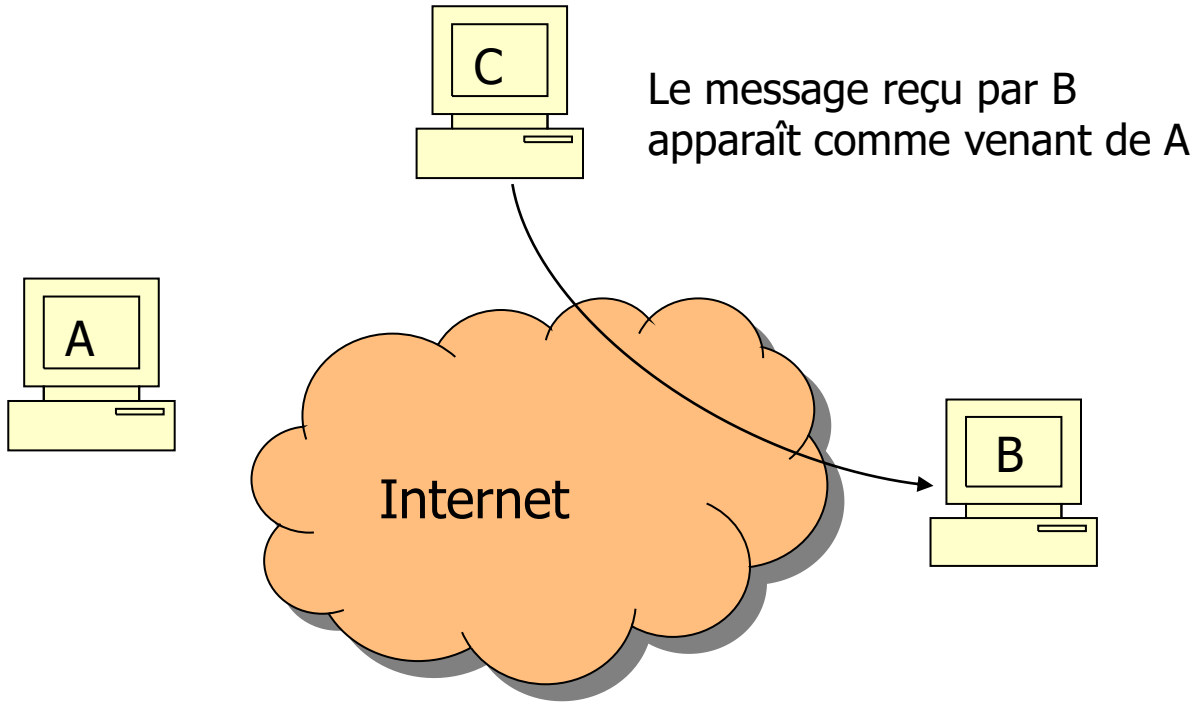
Quelques exemples des attaques passives

CAPTURE + ANALYSE DE TRAFIC : attaque passive



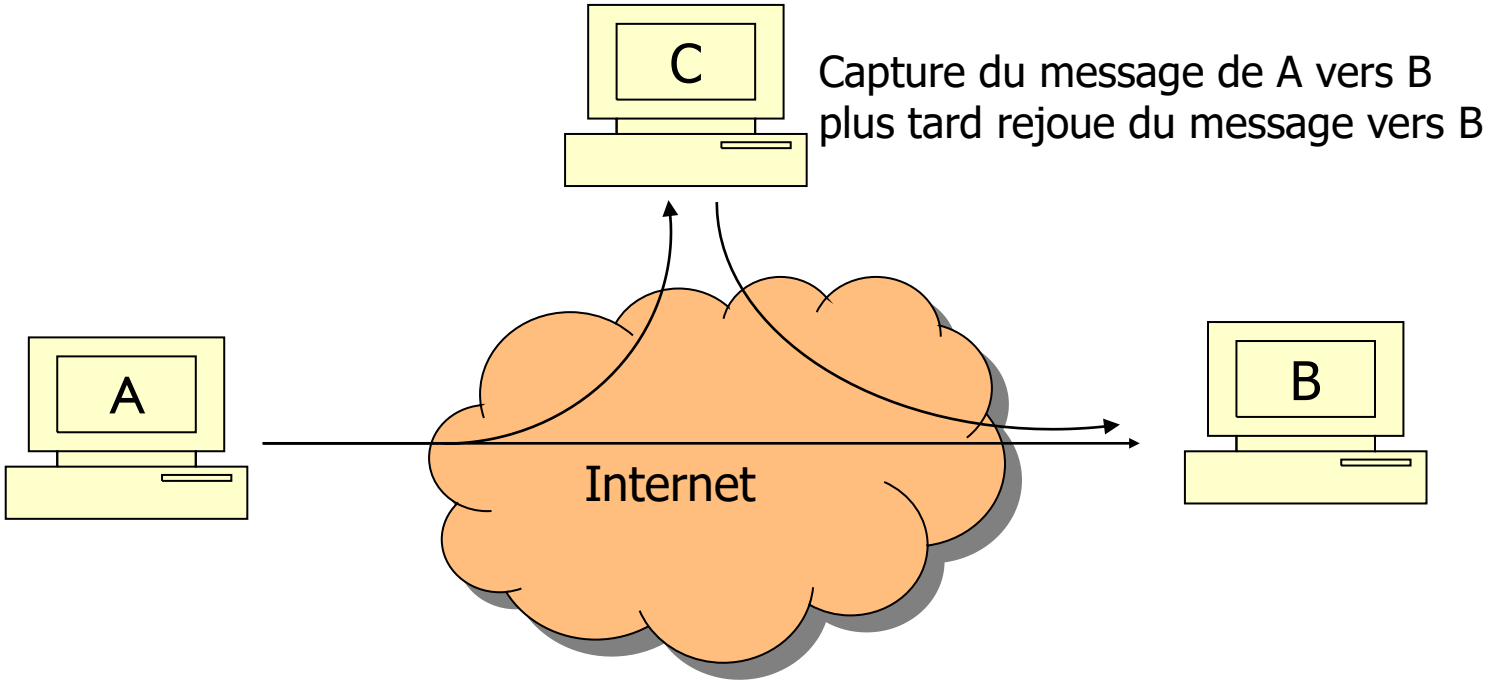
Quelques exemples des attaques actives

MASCARADE : attaque active



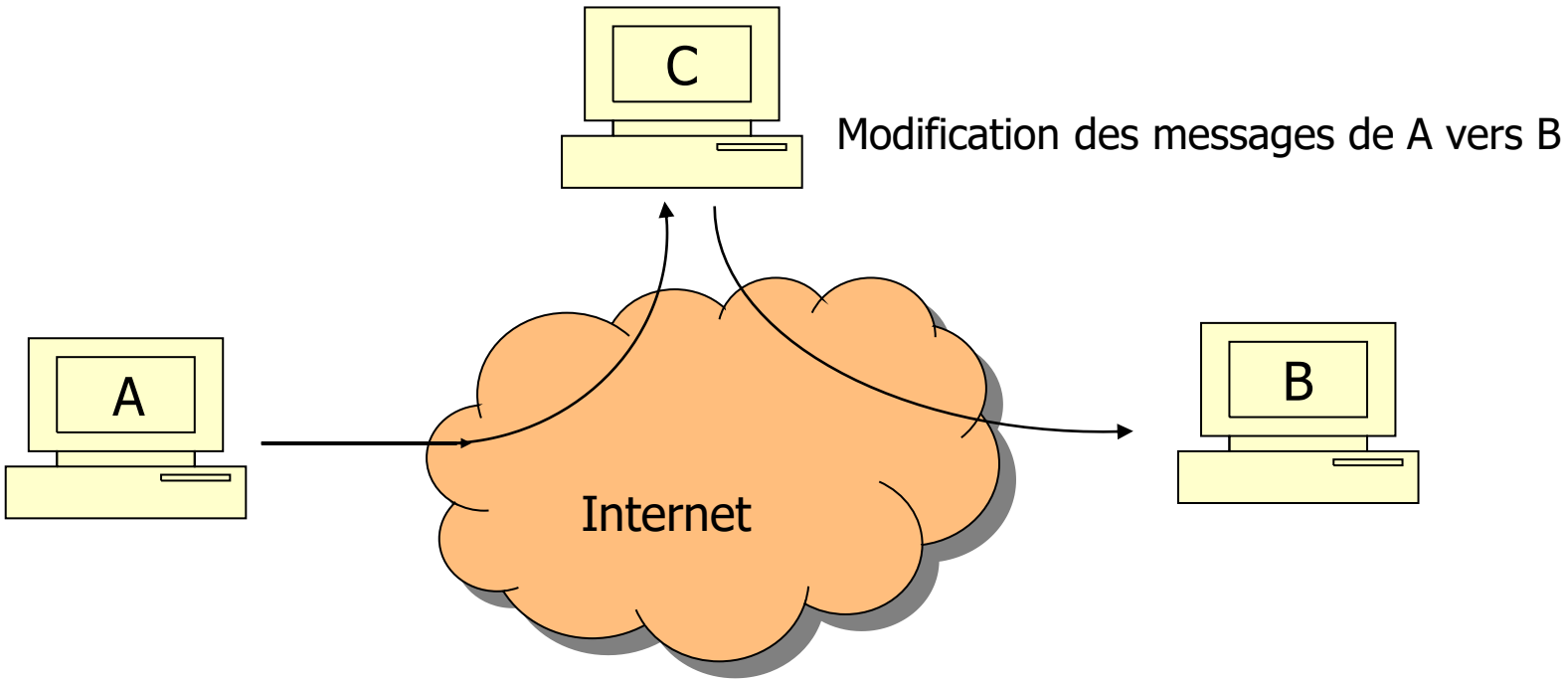
Quelques exemples des attaques actives

REJEU : attaque active



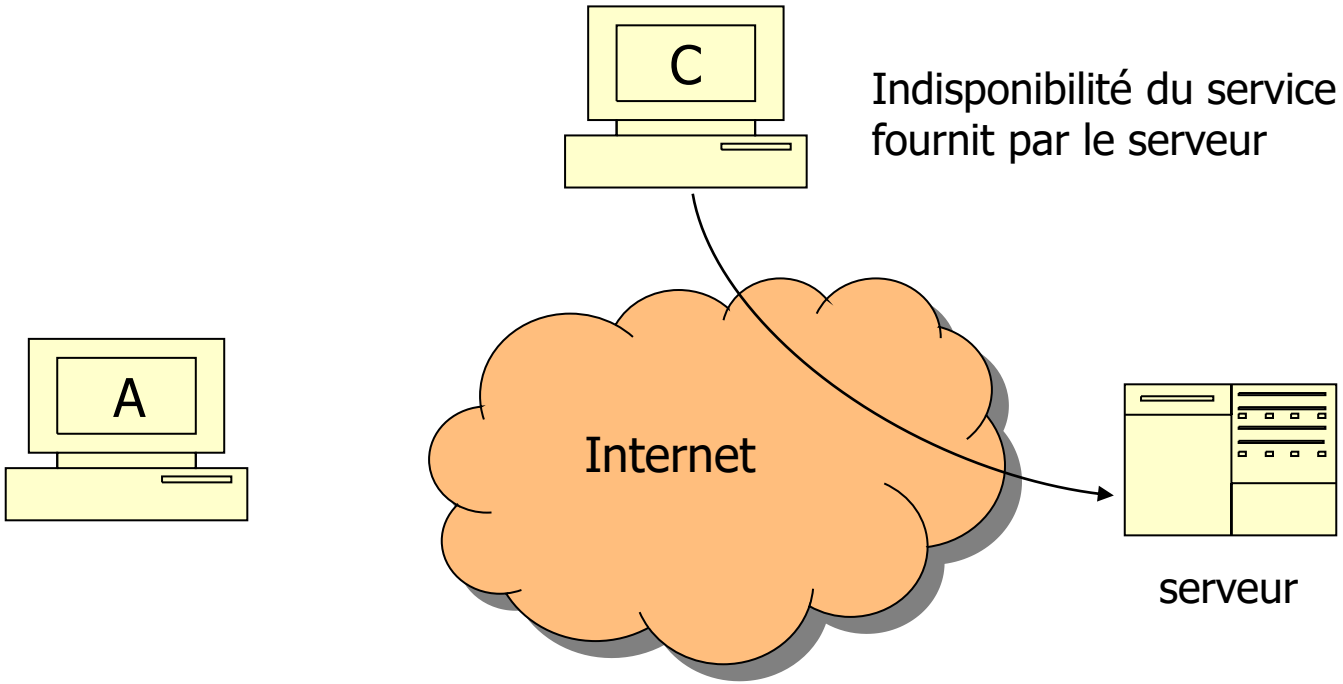
Quelques exemples des attaques actives

MODIFICATION : attaque active



Quelques exemples des attaques actives

DENI DE SERVICE : attaque active



Qui représente un danger ?

Des utilisateurs :

✓ 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

✓ Cracker : celui qui veut **casser** un système et causer des **dommages**

✓Les espions: Pirate payé par une entreprise ou un organisme concurrent pour **récolter** (de façon frauduleuse) des informations sur un domaine précis

Déroulement des attaques sur TCP/IP

- Recherche systématique d'informations
  - DNS, whois, moteurs de recherche
- Recherche de vulnérabilités connues à l'aide d'outils de *scan*
  - Services ouverts (SMTP, HTTP, etc), type de système d'exploitation
  - `traceroute, ping, firewalk, filterrules, nmap, queso, netcat, udp-scan`
- Tentative d'intrusion par exploitation des vulnérabilités
- Mise en place de portes dérobées, de systèmes d'écoute du réseau
- Tentative de suppression des traces
- Tentative de déni de service
- Prise de contrôle partielle ou totale du système distant

Méthodologie globale (1)

Les pirates (hackers) ayant l'intention de s'introduire dans les systèmes informatiques recherchent dans un premier temps des **failles (vulnérabilité)** dans:

- **les protocoles**,
- **les systèmes** d'exploitations,
- **les applications**
- **le personnel d**'une entreprise.

Les termes de **vulnérabilité** (**brèche** ou en langage plus familier **- trou de sécurité** « en anglais *security hole* ») sont également utilisés pour désigner les failles de sécurité.

Méthodologie globale (2)

- Pour pouvoir mettre en œuvre un **EXPLOIT(** il s'agit du terme technique signifiant *exploiter une vulnérabilité*), la première étape du pirate consiste à récupérer le maximum d'informations sur l'architecture du réseau et sur les systèmes d'exploitations et applications fonctionnant sur celui-ci. La plupart des attaques sont l'oeuvre de *script kiddies* essayant bêtement des exploits trouvés sur Internet, sans aucune connaissance du système, ni des risques liés à leur acte.

- Une fois que le pirate a établi une cartographie du système, il est en mesure de mettre en application des exploits relatifs aux versions des applications qu'il a recensées. Un premier accès à une machine lui permettra d'étendre son action afin de récupérer d'autres informations, et éventuellement d'étendre ses privilèges sur la machine.

Méthodologie globale (3)

- Lorsqu'un accès administrateur (le terme anglais ***root*** est généralement utilisé) est obtenu, on parle alors de compromission de la machine (ou plus exactement en anglais *root compromise*), car les fichiers systèmes sont susceptibles d'avoir été modifiés. Le pirate possède alors le plus haut niveau de droit sur la machine.

- S'il s'agit d'un pirate, la dernière étape consiste à **effacer ses traces**, afin d'éviter tout soupçon de la part de l'administrateur du réseau compromis et de telle manière à pouvoir garder le plus longtemps possible le contrôle des **machines compromises**.

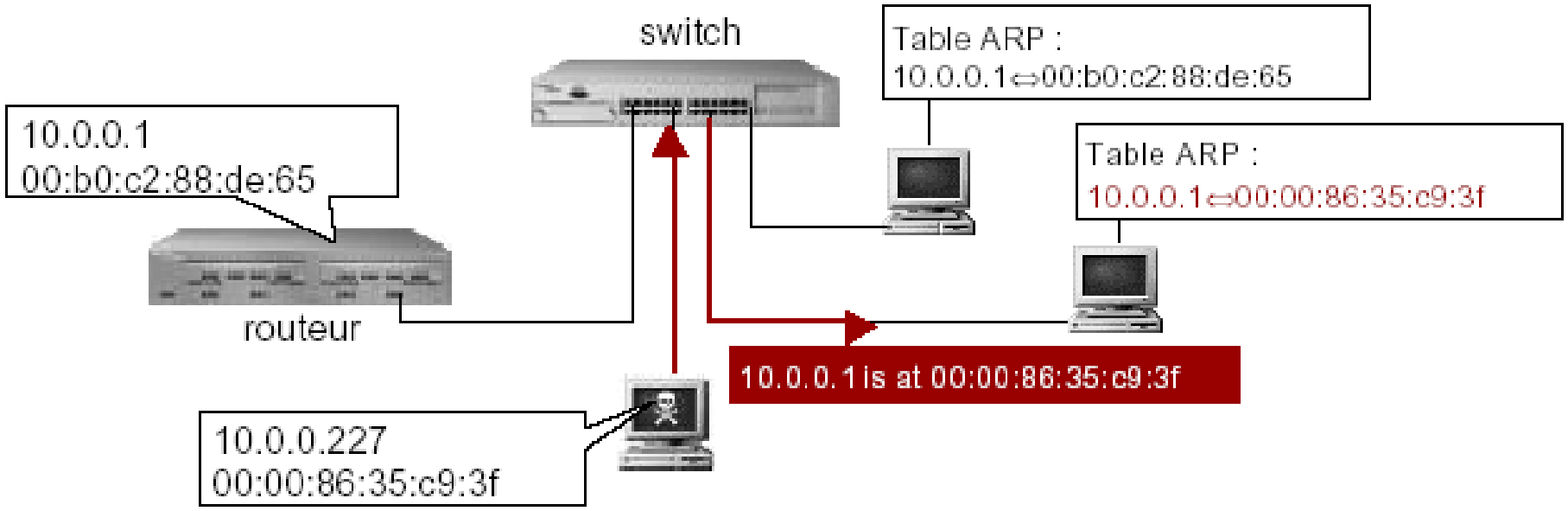
Balayage du réseau (Scan)

- Lorsque la topologie du réseau est connue par le pirate, il peut le scanner (le terme *balayer* est également utilisé), c'est-à-dire déterminer à l'aide d'un outil logiciel (appelé *scanner* ou *scanneur* en français) 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.

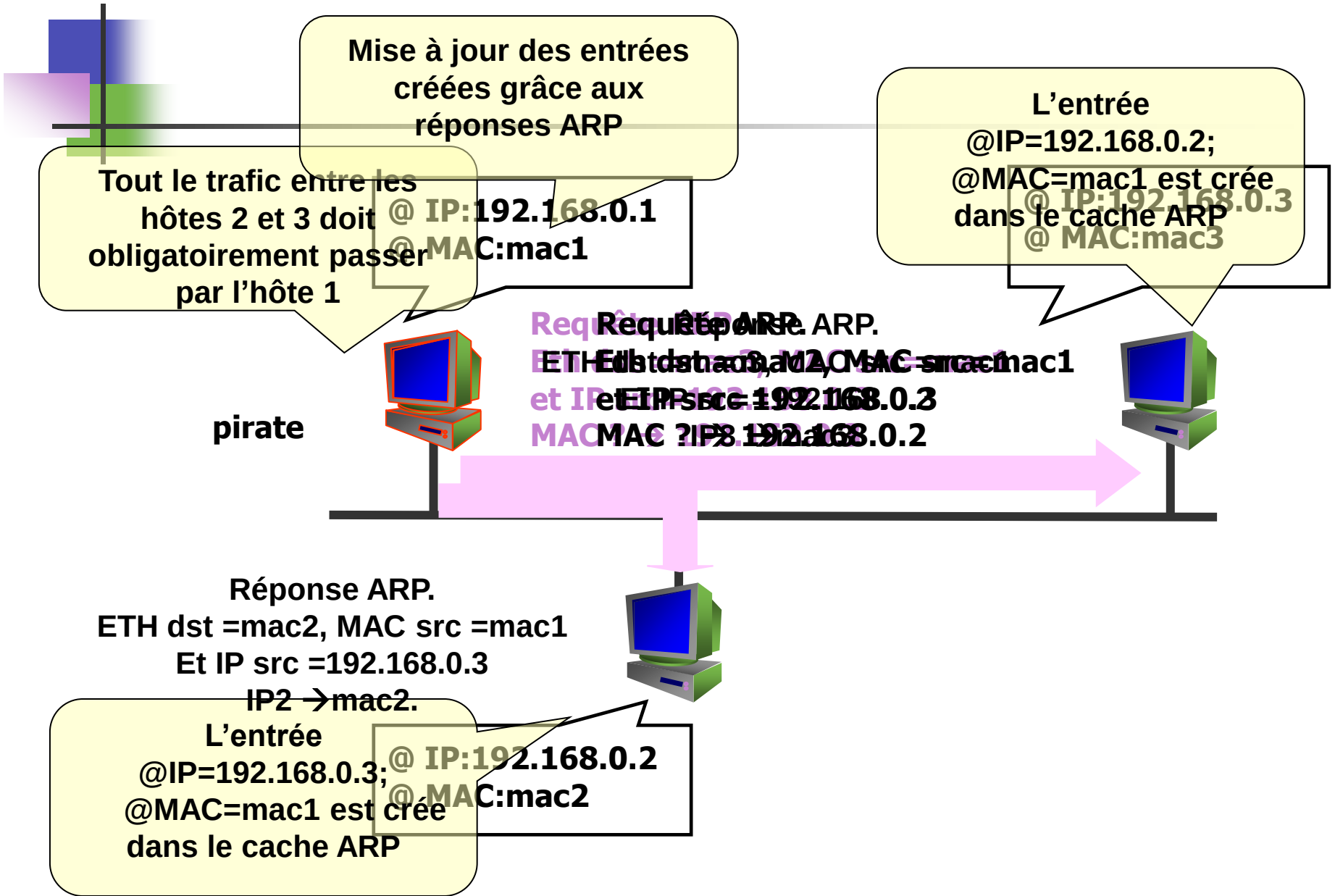
- L'un des outils les plus connus pour scanner un réseau est « **Nmap**», reconnu par de nombreux administrateurs réseaux comme un outil indispensable à la sécurisation d'un réseau. Cet outil agit en envoyant des paquets TCP et/ou UDP à un ensemble de machines sur un réseau (déterminé par une adresse réseau et un masque), puis il **analyse les réponses**. Selon l'allure des paquets TCP reçus, il lui est possible de déterminer le **système d'exploitation** distant pour chaque machine scannée.

ARP *spoofing*

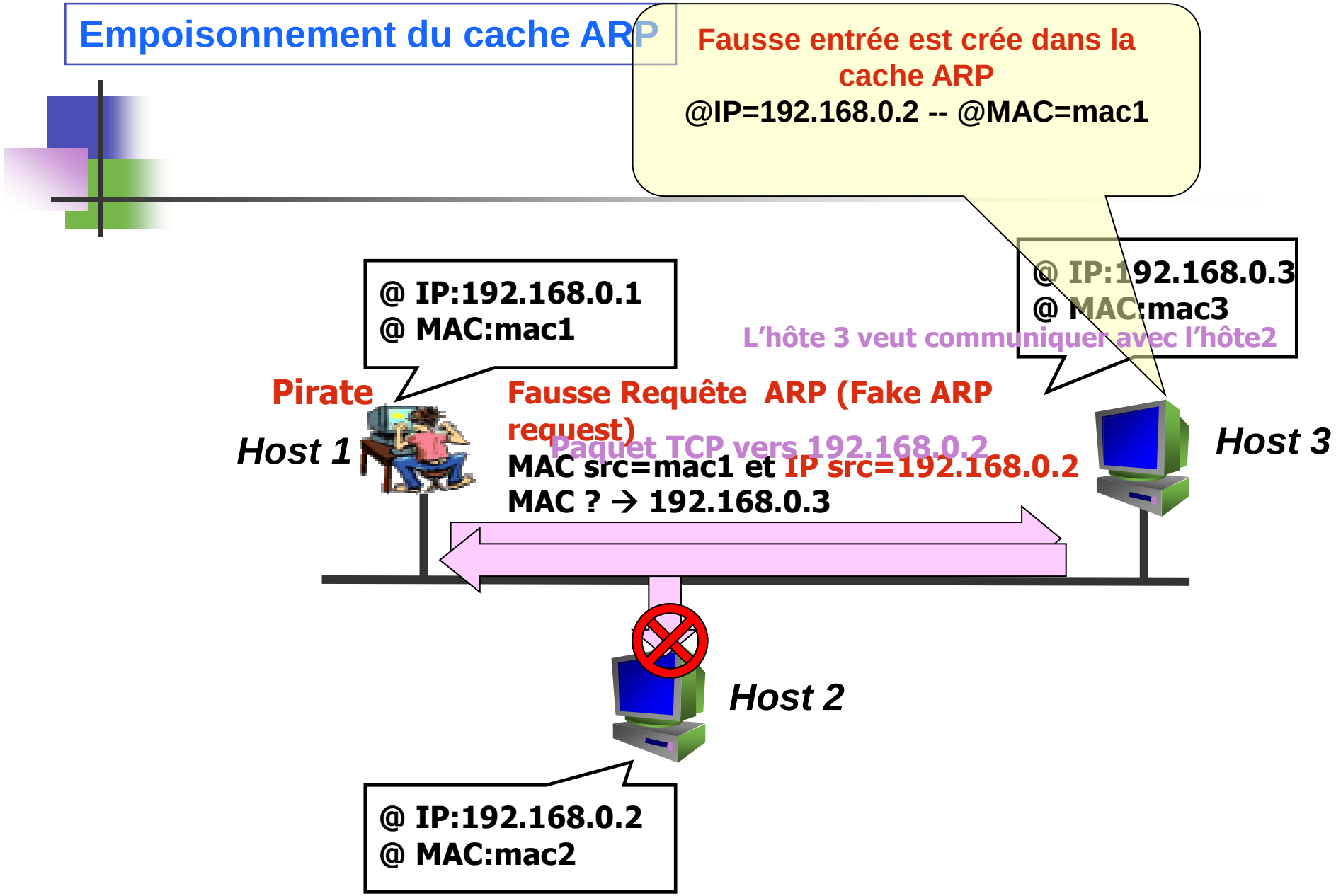
- Principe : rediriger le trafic réseau d'une ou plusieurs machines vers la machine du pirate, en corrompant le cache ARP
- S'effectue sur le réseau physique des victimes
- Sert lorsque le réseau local utilise des commutateurs (*switchs*) ➔ capture des trames impossible



Le principe de l'attaque « ARP cache poisoning »



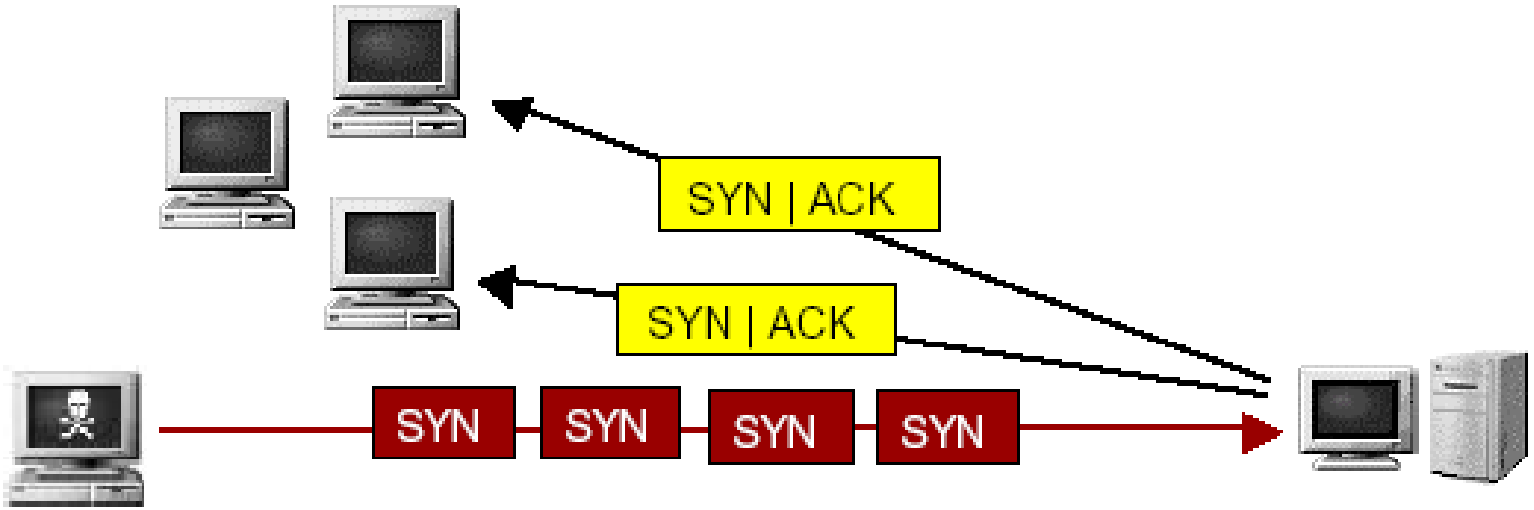
Empoisonnement du cache ARP



Inondation de SYN

(*SYN-flooding*)

- Principe : envoyer massivement des demandes de connexion (flag SYN à 1) vers la machine cible avec des adresses sources aléatoires
- La machine cible renvoie les SYN-ACK en réponse à chaque SYN reçu
- Aucun ACK n'est renvoyé pour établir la connexion : ces connexions semi-ouvertes consomment des ressources mémoire
- Au bout d'un moment, la machine cible est saturée et ne peut plus accepter de connexions



DNS Spoofing

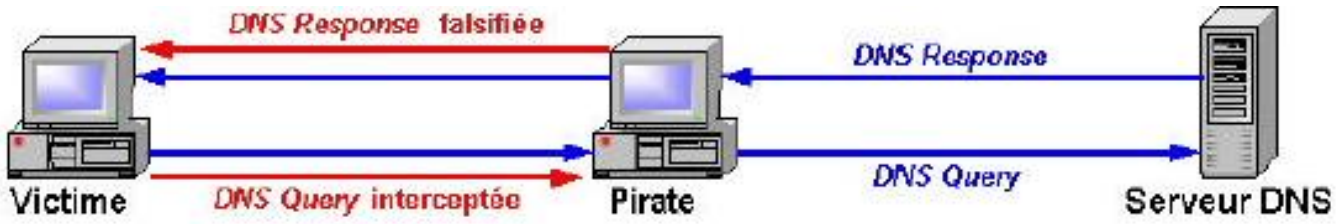
- DNS
  - Gestion des correspondance entre les noms de **machines** et leur adresse **IP**;
  - Un client lance une requête DNS au serveur pour connaître l'adresse IP à partir d'un **nom**. Le serveur lui répond par un paquet DNS;
  - La relation entre la requête et la réponse est une clé contenant un n° d'identification;
  - Ce protocole utilise le port UDP 53;

Attaque

- L'attaque **DNS Spoofing** est basée sur l'interception du paquet réponse, forger un nouveau avec la même clé et modifier l'adresse IP;
- Cette nouvelle adresse IP est une **redirection** sur la machine **pirate**;
- Il faut être positionné dans un environnement où il est possible de **sniffer** les paquets TCP. Éventuellement utiliser une attaque de type « ARP Cache Poisoning ».

Outil

- Pour ce genre d'attaque, un des outils est : **WinDNSSpoof**.



Les détournements et interceptions Web spoofing

- Attaque de type ***man in middle*** : le serveur de l 'attaquant détourne les requêtes HTTP de la victime
- La victime navigue dans un faux web
- Initialisation de l 'attaque:
  - l 'attaquant amène la victime à visiter son site (par email ou par sa figuration dans une indexation d 'un moteur de recherche)
  - la victime télécharger un script java
- Ce script java détourne toutes les requêtes de la victime vers l 'attaquant

MAITRISE ET CONTRÔLE DES FLUX RESEAU

Un flux est caractérisé par :

- une source,
- une destination
- un protocole d'échange

La topologie du réseau doit être adaptée à la réalisation du filtrage :

- regroupement des machines de même nature et de même niveau de sécurité (*poste de travail standard, poste d'administration, plate-forme de test, serveurs,…)*
- protection des segments de réseau (*accès physique aux prises murales, détection d'intrus, filtrage protocolaire,…)*

MAITRISE ET CONTRÔLE DES FLUX RESEAU (suite)

Pour implémenter une bonne sécurité, on doit disposer :

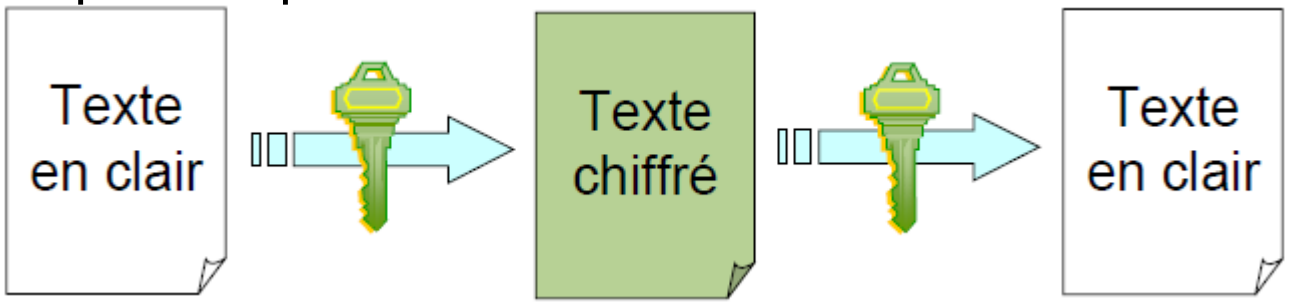
- d'une parfaite connaissance des flux qui vont transiter sur le réseau
- d'une organisation adaptée au contrôle
- d'une surveillance des filtres afin d'éviter la présence de filtres trop rigoureux ou trop ouverts
- d'une détection des tentatives d'intrusion
- de procédures d'exploitation adaptées au contexte et sécurisées

Principaux outils de défense (1/5)

Cryptographie :

→Technique utilisée pour assurer la **confidentialité** des informations

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



→Utilisée lors des échanges des informations ou pour minimiser les dégâts des vols(des ordinateurs portables, des disques,…)

Principaux outils de défense (2/5)

La signature numérique

→ Un moyen qui permet de garantir l'**intégrité** du message lors des échanges des données

→ Le principe de la *signature numérique* consiste à appliquer une fonction mathématique sur une portion du message qui est utilisé comme emprunte digitale pour ce message

Principaux outils de défense (3/5)

Firewalls :

→Un firewall est un système ou un groupe de système qui gère les **contrôles d'accès** entre deux réseaux

→Agit comme une barrière entre le réseau ***interne*** de l'entreprise et ***l'extérieur***

→ Protéger l'entreprise des ***intrus*** et des ***accès non identifiés***

Principaux outils de défense (4/5)

IDS (outil de Détection d'intrusion):

→Ce logiciel émet une **alarme** lorsqu'il détecte que quelqu'un de non-autorisé est entré sur le réseau

→Essaie de détecter toute **violation** de privilège interne ou externe

→Types des IDS:

-Les scanners des **vulnérabilités** testent la cible afin d'identifier quelles sont les **failles** connues du système

-Les IDS host : détectent des ***intrusions*** sur les hosts sur lesquels sont installés

-Les IDS network : observent le trafic réseau directement

Principaux outils de défense (5/5)

Serveur Proxy

Antivirus

Programme de test de vulnérabilité

...

Politique de sécurité (1/2)

→Ensemble de règles spécifiant:

-Comment les ressources sont gérées afin de satisfaire les exigences de la sécurité

- Quels sont les actions **permises** et les actions **interdites**

→ Objectif*: Empêcher les violations de sécurité telles que:* ***accès non autorisé***, **perte de données**, **interruption de services**, etc

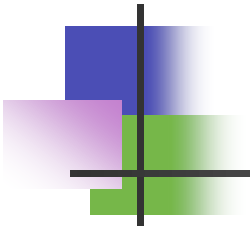
→Implémentation: Partiellement automatisée, mais toutes les personnes sont impliquées.

Politique de sécurité (2/2)

→Domaine d'application: Elle doit fixer l'ensemble du personnel qui doit la respecter et l'appliquer

→Domaine de responsabilité: administrateur système, …

→Définit les règles pour :
✓La gestion des **mots de passe**
✓ L'authentification des utilisateurs
✓ Le contrôle d'accès (réseau et système)
✓L'architecture du réseau
✓ La sécurité du personnel (formation, …)
✓ La sécurité physique, etc.
✓…



Partie II: Audit des systèmes informatiques

Plan

- Definitions
- Objectifs de l'audit informatique
- Travaux de l'audit informatique
- Les outils de l'auditeur informatique

Définitions

Audit

→L'audit est **l'examen** d'une situation, d'un **système d'informations**, d'une organisation pour porter un **jugement**

→C'est la **comparaison** entre ce qui est **observé** et ce que cela **devrait être**, selon un système de références.

Audit informatique

→l'audit informatique apporte :

-Un **conseil** en organisation fourni par des **spécialistes extérieurs**

-Le moyen d'accompagner et de justifier la **mise en place** de nouvelles structures ou de nouvelles méthodes

Les objectifs de l'audit informatique

l'audit informatique concerne :

✓ Les aspects stratégiques : conception et planification de la mise en œuvre du système d'informations

✓ L'environnement et l'organisation générale de la gestion de l'informatique

✓ Les activités courantes de gestion de l'informatique

✓ Les ressources informatiques mises en service

✓Les applications informatiques en service

✓La sécurité

Travaux D'audit informatique

Mission

Evaluer:

- ✓L'infrastructure informatique
- ✓Une application informatique
- ✓Un système ou une application informatique en cours de réalisation
- ✓…

Livrable

- ✓**Rapports** contenant les **faiblesses** relevées
- ✓**Mesures** proposées pour réduire et contrôles des **risques** des nouveaux systèmes
- ✓…

Les outils de l'auditeur informatique

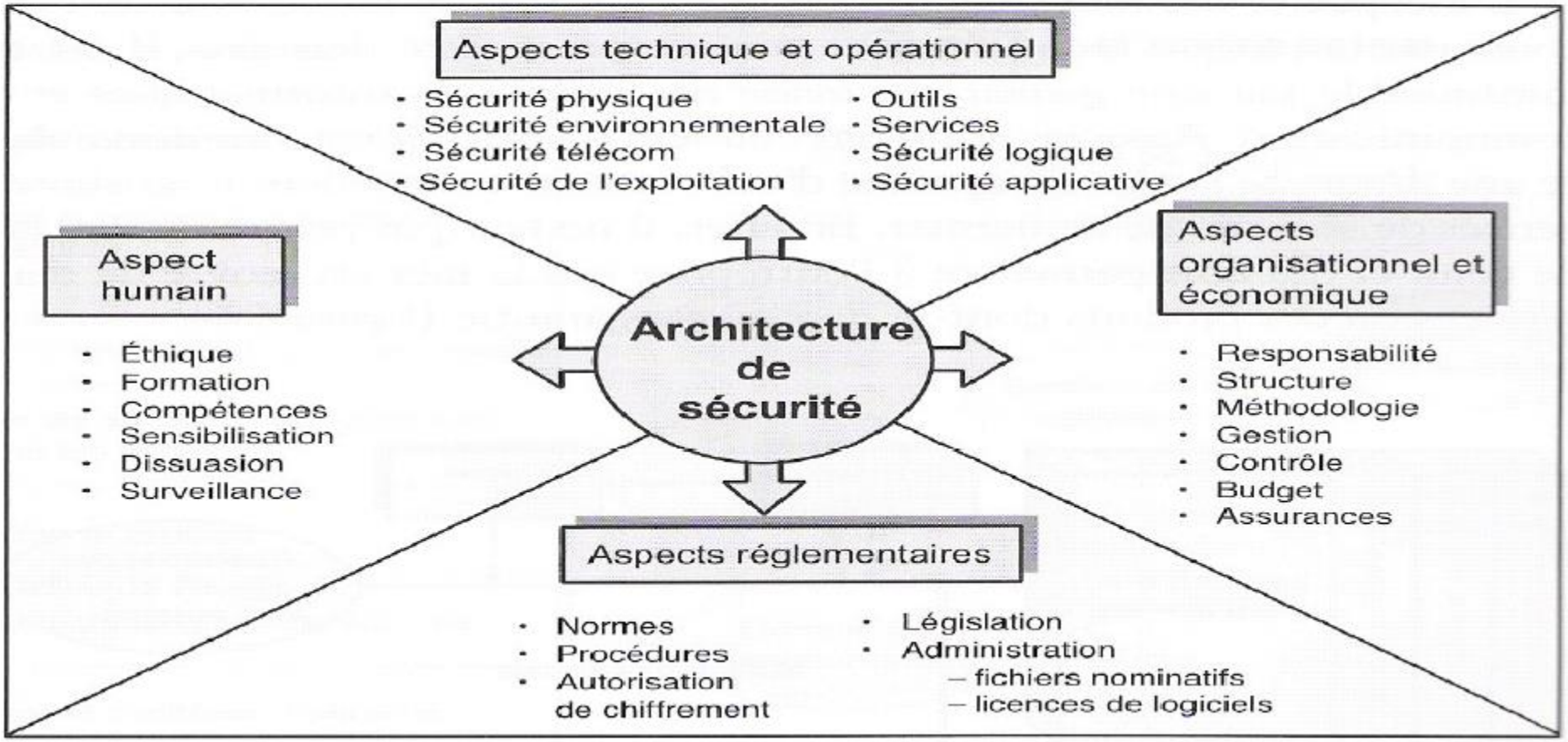
→L'auditeur informatique peut disposer de deux types d'outils importants dans le cadre de son activité :

- ✓ Les **méthodes d'analyse** des risques informatiques
- ✓ Les **progiciels** d'audit

Synthèse

- Aucune sécurité n'est **parfaite**
- Des outils sont nécessaires, mais **le travail quotidien** est indispensable
- La sécurité n'apporte qu'un gain indirect. Par conséquent, il n'est pas facile de convaincre **les décideurs** de l'entreprise
- Le seul système informatique qui est vraiment sûr est un système éteint et débranché, enfermé dans un blockhaus sous terre, entouré par des gaz mortels et des gardiens hautement payés et armés.

Les différents aspects d'une architecture de sécurité



Évaluer sa sécurité : outils

- SATAN
  - Security Analysis Tool for Auditing Networks
  - Package logiciel comprenant
    - Pages HTML pour l'interface et la documentation,
    - Scripts Perl pour la collecte d'informations et l'analyse,
    - Programmes C de tests.
  - Détection de machines et de réseaux,
  - Détection des services disponibles,
  - Détection de bugs connus,
  - Analyse des résultats
    - Par machine,
    - Par réseau,
    - Par service,
    - Par application vulnérable (bug).

Évaluer sa sécurité : outils

- COPS
  - Computer Oracle and Password System
  - Ensemble de programmes qui vérifient ou détectent :
    - Les permissions de certains fichiers, répertoires,
    - Les mots de passe,
    - Le contenu des fichiers passwd et group,
    - Les programmes lancés dans etc/rc et cron,
    - Les fichiers SUID root,
    - L'accès à certains fichiers (.profile,.cshrc…),
    - L'installation correcte de ftp anonyme,
    - Certains trous de sécurité (montage NFS…).
  - Audit de sécurité sur une machine UNIX
  - Peut être exécuté sans être root

Évaluer sa sécurité : outils

- Internet Scanner Safe suite
  - Suite logicielle d'audit pour tester la sécurité réseau,
  - Test de 140 vulnérabilités,
  - Scan des sites Web, firewalls, routeurs, serveurs NT et Unix, périphériques TCP/IP,
  - Recommandation des corrections appropriées,
  - Configurable et automatisable,
    - Planification périodique des scans,
    - Priorité de niveaux de vulnérabilité,
    - Etc.

Évaluer sa sécurité : outils

- Les deux principaux scanneurs de failles sont : Nessus et SAINT