Sécurité des réseaux

Licence DA2I

Sources d'inspiration

- Jean-Christophe GALLARD, CNAM, Sécurité et Réseaux http://jgallard.free.fr/RSX112.pdf.
- Bernard Cousin, Université de Rennes 1, Sécurité des réseaux informatiques, *www.irisa.fr/prive/bcousin/.../1-Securite-des-reseaux.2P.pdf*

Sécurité et Internet

- Internet vous permet de se connecter à des millions d'ordinateurs …
- … mais ces ordinateurs peuvent aussi se connecter à vous !
- Plusieurs point d'accès au réseau: téléphone, Ethernet, x25, Wireless, etc..
- Culture de système ouvert

Définitions: Attaques, Services et Mécanismes

- **Une Attaque :** n'importe quelle action qui compromet la sécurité des informations.
- **Mécanismes de Sécurité :** un mécanisme qui est conçu pour détecter, prévenir et lutter contre une attaque de sécurité.
- **Service de Sécurité :** un service qui augmente la sécurité des traitements et des échanges de données d'un système. Un service de sécurité utilise un ou plusieurs mécanismes de sécurité.

Les attaques

- Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.
- Une «attaque» est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel, erreur de configuration, etc.) à des fins non connues par l'exploitant du système et généralement préjudiciables.
- Sur l'Internet:
  - des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée.
  - Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire et aussi par l'action de pirates informatiques.

Les attaques: types d'attaque

On peut classiquement définir **deux grands types d'attaque** sur les réseaux : les attaques sur *les protocoles de communications*, d'une part, et les attaques sur *les applications standards*, d'autre part.

- Les attaques sur les protocoles de communications consistent pour un agresseur à profiter des failles des protocoles de communications (IP, ICMP, TCP et UDP pour l'essentiel).
- L'autre volet bénéficie des vulnérabilités des applications classiques mises en œuvre dans les Intranets et les Extranets (HTTP, SMTP, FTP…).
- On peut également distinguer les attaques sur l'information elle-même des attaques sur les systèmes d'informations.
  - le premier cas atteint l'intégrité / disponibilité / confidentialité aux données traitées par les systèmes (par le biais de virus, d'écoute réseau, de modifications de données…),
  - le second cas de figure vise à se ménager une porte d'entrée dans les systèmes traitant les données (vols de mots de passe, exécution de processus non autorisés, a…).

Buts des attaques

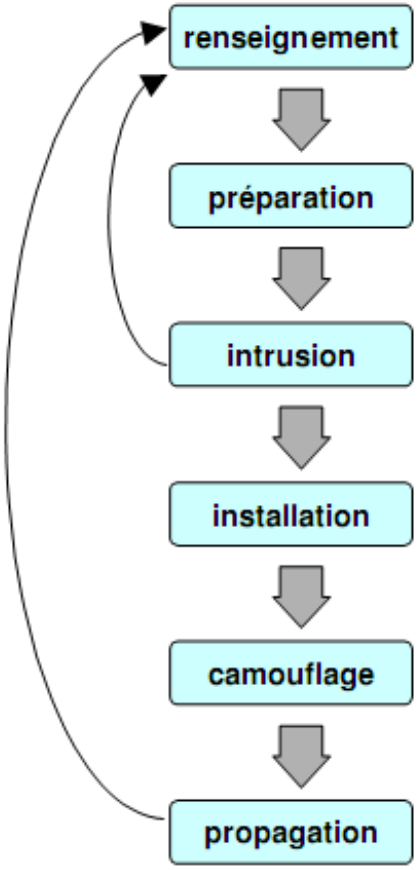
- **Interruption:** vise la disponibilité des informations
- **Interception:** vise la confidentialité des informations
- **Modification:** vise l'intégrité des informations
- **Fabrication:** vise l'authenticité des informations

Scénario d'une intrusion

- Généralement le 'vilain intrus':
  - Localise un système à attaquer (nouveau système, …)
  - Gagne l'entrée à un compte utilisateur
  - Exploite les insuffisances de configuration du système ou la vulnérabilité des logiciels pour accéder à un compte privilégié
  - Supprime les traces d'intrusion
  - Fait des activités non autorisées
  - Installe des "*back doors*" pour une utilisation ultérieure
  - Installe un "Cheval de Troie" (*Torjan horse*) ou *'packet snifer'* pour capter tout ce qui se passe sur le système.
  - Saute sur d'autres ressources du réseau local.

Scénario d'une intrusion

Un scénario d'intrusion sur un système peut se décomposer en six actions élémentaires, enchaînées selon un processus itératif :



découvrir l'architecture du système, son plan d'adressage
écoute, furetage, espionnage, cryptanalyse

dégrader ou contourner la sécurité
leurrage, sabotage, bombe logique, parasitage, saturation

entrer par un point faible
usurpation de nom, d'adresse, cheval de Troie, essais exhaustifs

installer une entrée permanente
porte dérobée, **canal caché**

cacher l'entrée permanente
cacher les répertoires et fichiers pirates, inhiber la surveillance

attaquer les machines ou systèmes en mutuelle confiance
rebond IP ou X25, rhosts, domaines WinNT, virus, ver

Renseignement

- Dans tout scénario d'intrusion, l'identification précise de la cible est un pré-requis indispensable à la bonne conduite des agressions à venir.
- Le futur agresseur aura donc à cœur d'identifier le plus précisément possible les éléments matériels et logiques composant le système d'information.
- Ces investigations peuvent être mises en œuvre passivement au travers de sources ouvertes (sites Internet, presse, plaquettes de présentations…) puis complétées par des investigations plus actives allant de la simple écoute d'un réseau à l'espionnage industriel pur et simple.

Préparation

- La phase de préparation est à distinguer de celle du renseignement dans la mesure où il est surtout ici question de s'outiller correctement au vu des résultats des investigations précédentes.
- Le ciblage préalable permet adaptation active, où l'agresseur sélectionnera les actions futures qui ont le plus de chances d'aboutir à une intrusion sur le système considéré.
- Si, dans la phase de renseignement, l'agresseur aura pu repérer la présence de certains services pouvant potentiellement présenter des vulnérabilités (serveurs HTTP, accès de maintenance, équipements de réseau obsolètes, etc.) ce dernier ira donc chercher tout ce qu'il peut collecter sur les vulnérabilités de ses services.

Intrusion

- Il s'agit ici de la partie la plus « active », au cours de laquelle l'agresseur met en œuvre de manière effective les attaques pouvant potentiellement mener à la compromission du système visé.
- Les techniques utilisées ici dépendent très étroitement du système cible, d'où l'importance de renseignements les plus précis possibles en phases initiales.
- Parmi les techniques les plus couramment utilisées, on peut cependant citer :
  - Utilisation de bugs dans les services réseaux,
  - Exploitation d'une mauvaise configuration des systèmes (comptes sans mot de passe, systèmes déverrouillés « parce que ça marche mieux comme ça », …),
  - Branchement physique « pirate » sur une infrastructure de communication,
  - Utilisation des particularités des protocoles réseaux (usurpation d'adresse et / ou d'identité…).

Installation

- Suite à une intrusion réussie, un agresseur tentera alors de mettre en place dans le système un ensemble de mécanismes lui assurant une entrée permanente.
- L'agresseur tente d'installer une porte dérobée lui permettant de revenir discrètement sur sa cible le plus facile.
- Les techniques utilisées ici sont variées et plus ou moins discrètes : ajout d'un compte illicite, altération du filtrage réseau, service additionnel, shell distant,…

Camouflage

- Le principe de ce stade consiste à camoufler ses actions sur le système afin de les dissimuler aux administrateurs systèmes :

  - il est souvent étroitement lié à la phase d'installation (les deux phases sont par ailleurs souvent confondues) : fichiers et répertoires cachés, utilisation de noms de programmes insignifiant pour cacher ses portes dérobées, stockages hors norme, effacement et inhibition des journaux d'audit, altération des commandes systèmes (*ps*, *ls par exemple*)...

Propagation

- L'intrusion dans un système demeure souvent réalisée de façon unitaire, unité par unité. le plus souvent, l'intrusion sera réalisée sur une machine particulièrement vulnérable (serveur Web, serveur de messagerie, routeur d'accès…).

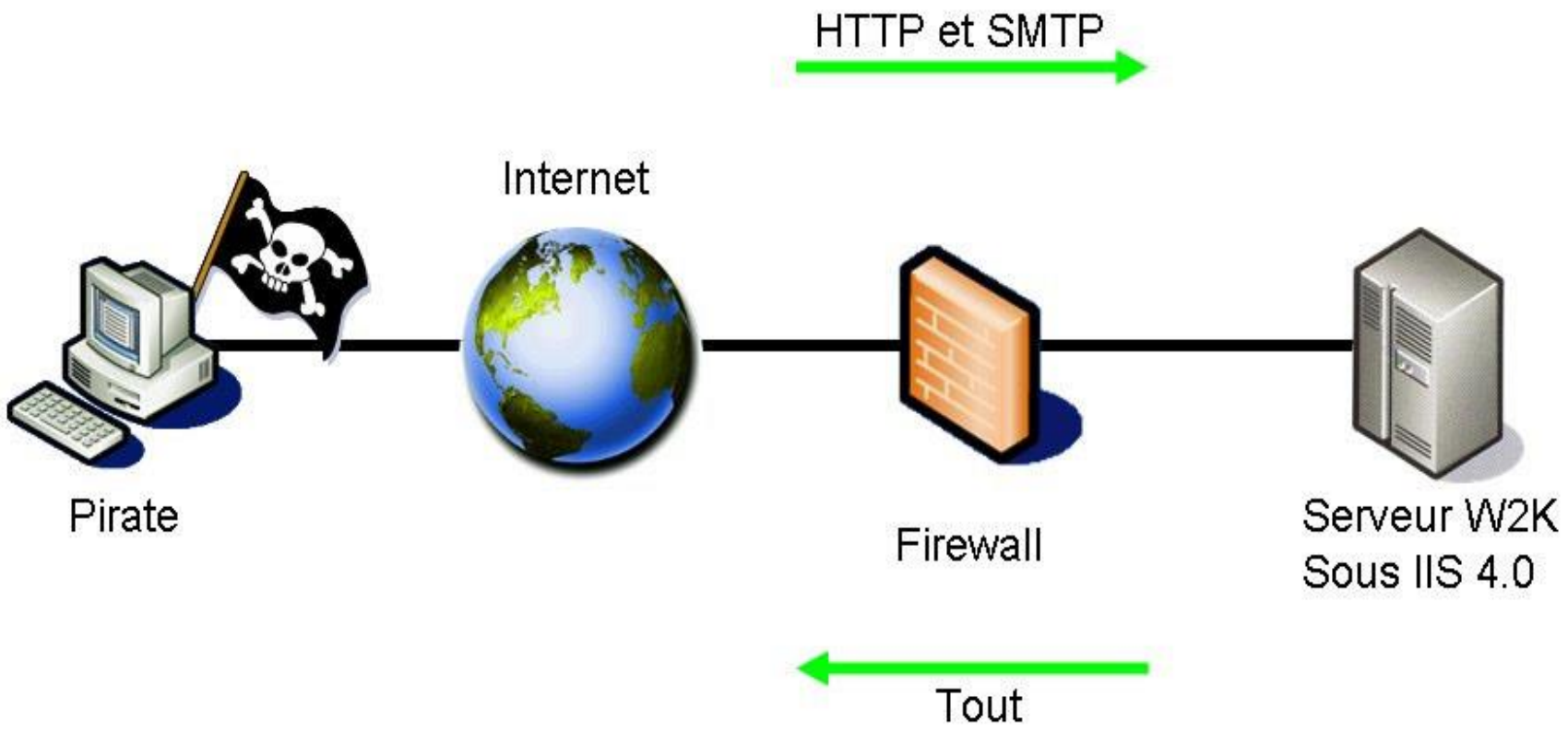
- L'agresseur tentera de propager son intrusion à d'autres éléments du système d'information, jusqu'ici inaccessibles.

- Cette propagation peut également intervenir sur d'autres systèmes distants.

Exemple de scénario d'intrusion

- Dans l'exemple qui suit, nous supposerons qu'un agresseur décide de s'attaquer à un serveur Web d'une entreprise sur l'Internet.
- Le serveur Web est un système Windows 2000 utilisant le service Web IIS (Internet Information Service) de Microsoft en version 4.0. Ce dernier est protégé de l'Internet par un Firewall dont les règles de filtrage :
  - autorisent le trafic HTTP (port 80) de l'Internet vers le serveur Web,
  - autorisent le trafic SMTP (port 25) de l'Internet vers le serveur Web (il s'agit ici d'une erreur de configuration, le serveur n'est pas censé héberger un service de messagerie),
  - autorisent tout trafic du serveur vers l'Internet,
  - Interdisent tout le reste.

Exemple de scénario d'intrusion



Exemple de scénario d'intrusion: Renseignement

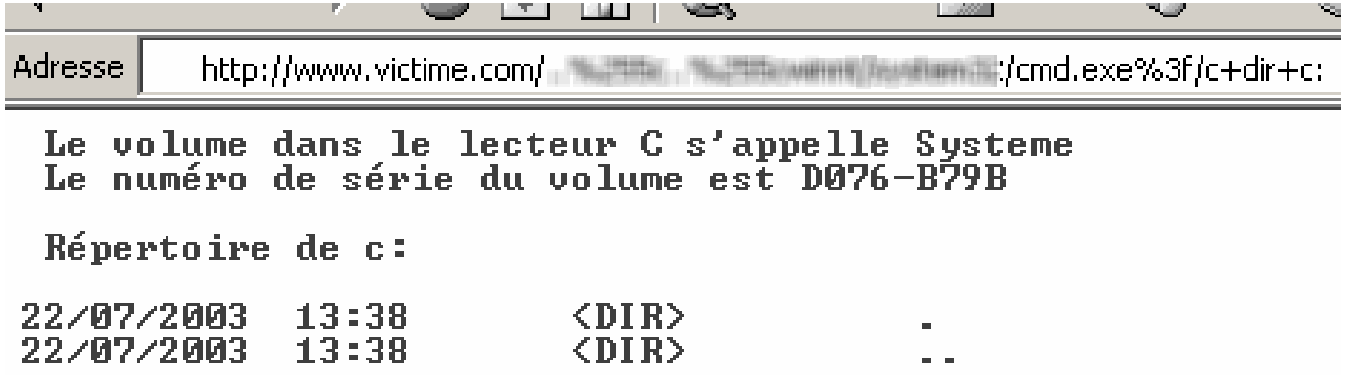
- Par navigation sur l'Internet, l'agresseur repère un lien sur un site vers notre serveur. Il dispose alors de son adresse (ou du moins de son nom, ce qui revient au même).
- L'agresseur réalise alors un « *port scanning* » à l'aide d'un outil comme *nmap*, en activant l'option de détection de système d'exploitation.
- nmap lui indique alors :
  - Que seul le port 80 est ouvert (donc qu'il existe un serveur Web),
  - Que la machine cible est une machine sous Windows (résultat de la détection de système d'exploitation),
  - Que le port 25 n'est pas filtré.
- En poursuivant ses investigations, il repère que le service Web est un service IIS en version 4.0 (par exemple par analyse des bannières HTTP lors d'une connexion sur ce service).

Exemple de scénario d'intrusion: Préparation

- Durant cette phase, l'agresseur va alors récupérer un maximum d'informations sur les vulnérabilités des serveurs sous IIS 4.0 en se connectant à des sites spécialisés. En particulier, il repère une vulnérabilité majeure lui permettant de lancer une commande à distance en utilisant un simple navigateur et une URL un peu particulière.
- Il en profite également pour récupérer un programme « cheval de Troie » permettant d'obtenir une invite de commande à distance sur la cible et écoutant sur le port 25.

Exemple de scénario d'intrusion: l' Intrusion (1)

- A l'aide de son navigateur, l'agresseur tente une connexion HTTP avec l'URL particulière en question, et en tentant de lister le contenu du répertoire C:\WINNT:



Le résultat de cette action s'affiche dans la fenêtre de son navigateur, lui indiquant que la vulnérabilité est exploitable sur ce système.

Après avoir créé un serveur TFTP sur sa propre machine et avoir déposé dans l'arborescence TFTP le fichier Troie.exe, il provoque le téléchargement de ce fichier sur le serveur Web en lançant une commande tftp sur le serveur :

Exemple de scénario d'intrusion: l'Intrusion (2)

- La copie s'étant correctement passée, il lance alors de la même manière son cheval de Troie sur le serveur, puis se connecte avec Telnet sur le port 25 de la victime et obtient alors une invite de commande distante.

Dès à présent, l'attaquant à tout loisir d'inspecter plus finement sa cible puisque qu'il se trouve désormais dans la place : il pourra ainsi repartir sur une phase de renseignement afin par exemple de détecter d'autres éventuelles vulnérabilités.

Exemple de scénario d'intrusion: suite

Installation

- La procédure suivie au préalable étant longue, l'agresseur rapatrie des outils plus sophistiqués sur le serveur victime de l'intrusion et installe ainsi une porte dérobée permanente qui lui évitera de devoir passer par la suite par le service Web pour s'introduire sur le serveur.

Camouflage

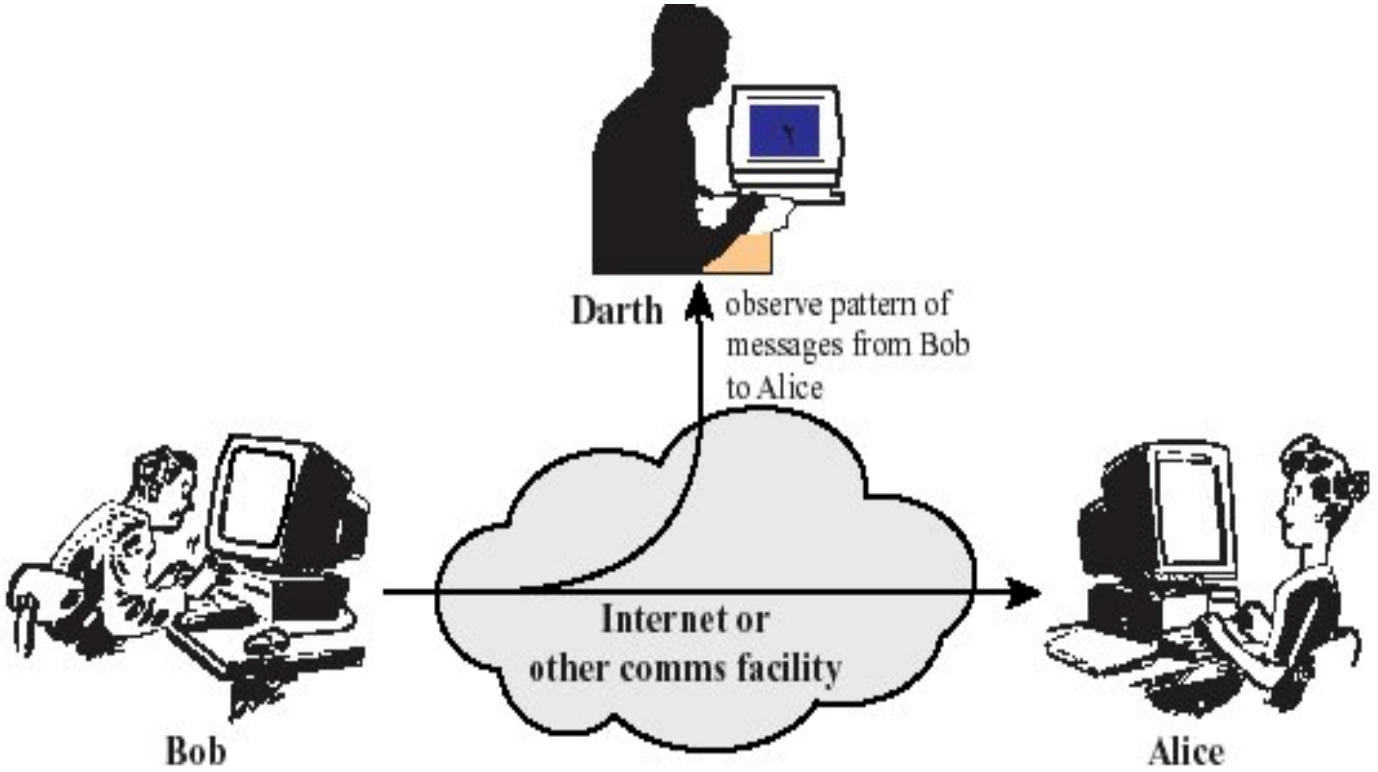
- L'entrée permanente est stockée dans l'arborescence système, sous un nom anodin et à l'apparence indispensable au fonctionnement du système (lsasrvsys32.exe par exemple). Les journaux d'événements du système sont également purgés.

Propagation

- Dès cet instant, l'attaquant peut alors utiliser cette machine corrompue comme système de rebond, soit pour atteindre des machines situées derrière le Firewall, mais jusqu'ici inaccessibles, soit pour attaquer d'autres sites Internet.

Description des attaques : analyse de trafic

IP Sniffing: Le principe de l'IP sniffing consiste pour un agresseur à écouter les trames circulant sur son segment réseau puis à les décoder, protocole par protocole, couche par couche.



Description des attaques : analyse de trafic

De nombreuses techniques peuvent être mises en œuvre pour réaliser cette opération d'usurpation d'identité d'une machine:

- Modification de l'adresse IP d'une machine.
- Modification de l'adresse hardware d'une station de travail (adresse MAC).
- Compromission d'un serveur DNS pour rediriger une requête DNS vers une station contrôlée par un intrus.
- Introduction de segments TCP avec des numéros de séquence appropriés dans une connexion.
- …

IP Sniffing:

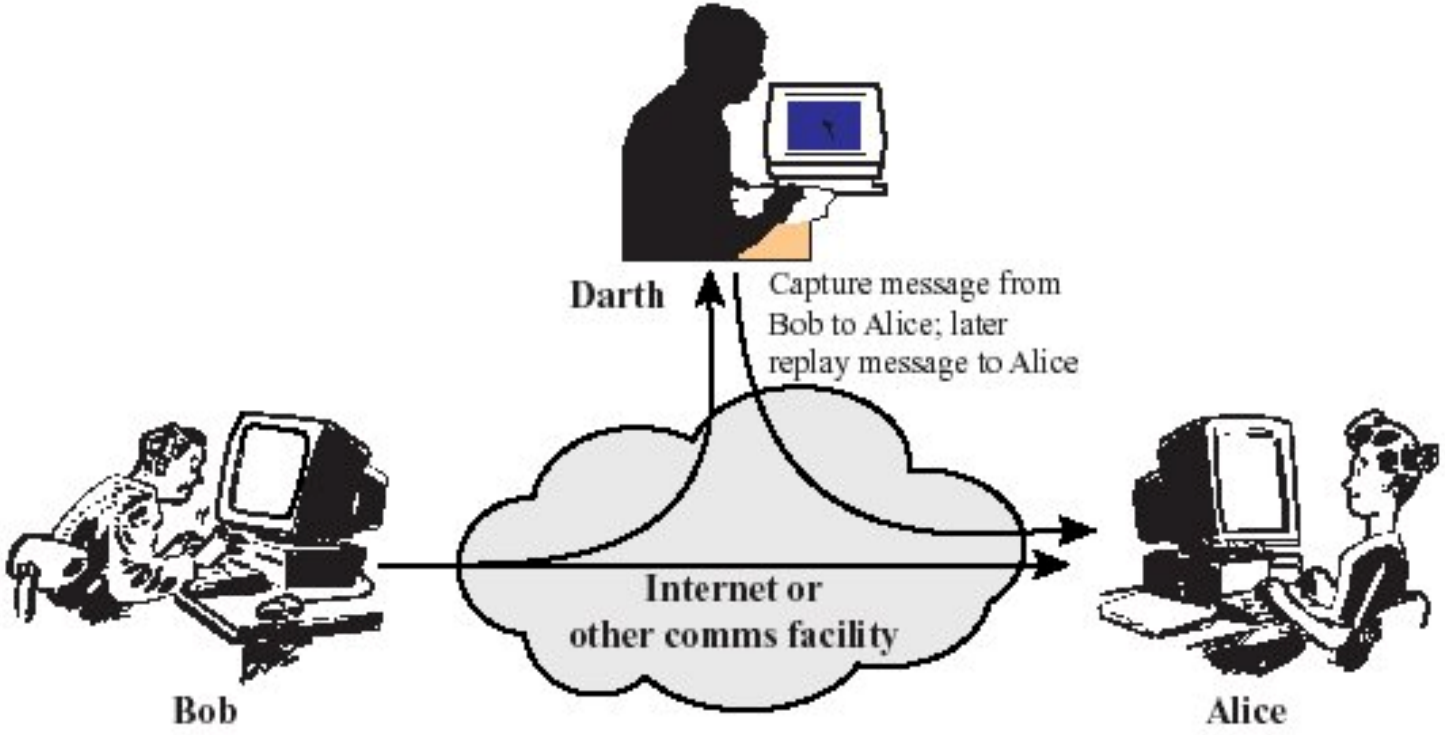
- Il s'agit principalement d'une méthode passive (les trames ne sont pas modifiées par cette opération).
- essentiellement utilisée pour atteindre en confidentialité à l'information.
- On l'utilise pour ce faire des outils de type «analyseurs réseaux»:
  - soit spécifiques à une action particulière (cas des analyseurs spécifiquement développés pour extraire des mots de passe en clair transitant sur le réseau),
  - soit généralistes (Ethereal, tcpdump…) mais détournés de leur fonction initiale (à savoir l'analyse des problèmes réseaux).
- La technique de snif ne peut être mise en œuvre que si l'on satisfait à l'une des deux conditions suivantes :
  - L'agresseur doit être situé sur le chemin réseau entre le client et le serveur,
  - Le segment réseau doit utiliser une technologie à diffusion (token ring ou Ethernet dans leurs concepts initiaux par exemple)

Description des attaques : IP Spoofing

L'IP Spoofing consiste à falsifier son adresse IP pour faire passer sa propre machine pour une autre. L'IP spoofing est souvent utilisé par des attaquants pour bénéficier des mécanismes de confiances qui peuvent être mis en œuvre dans certains systèmes.

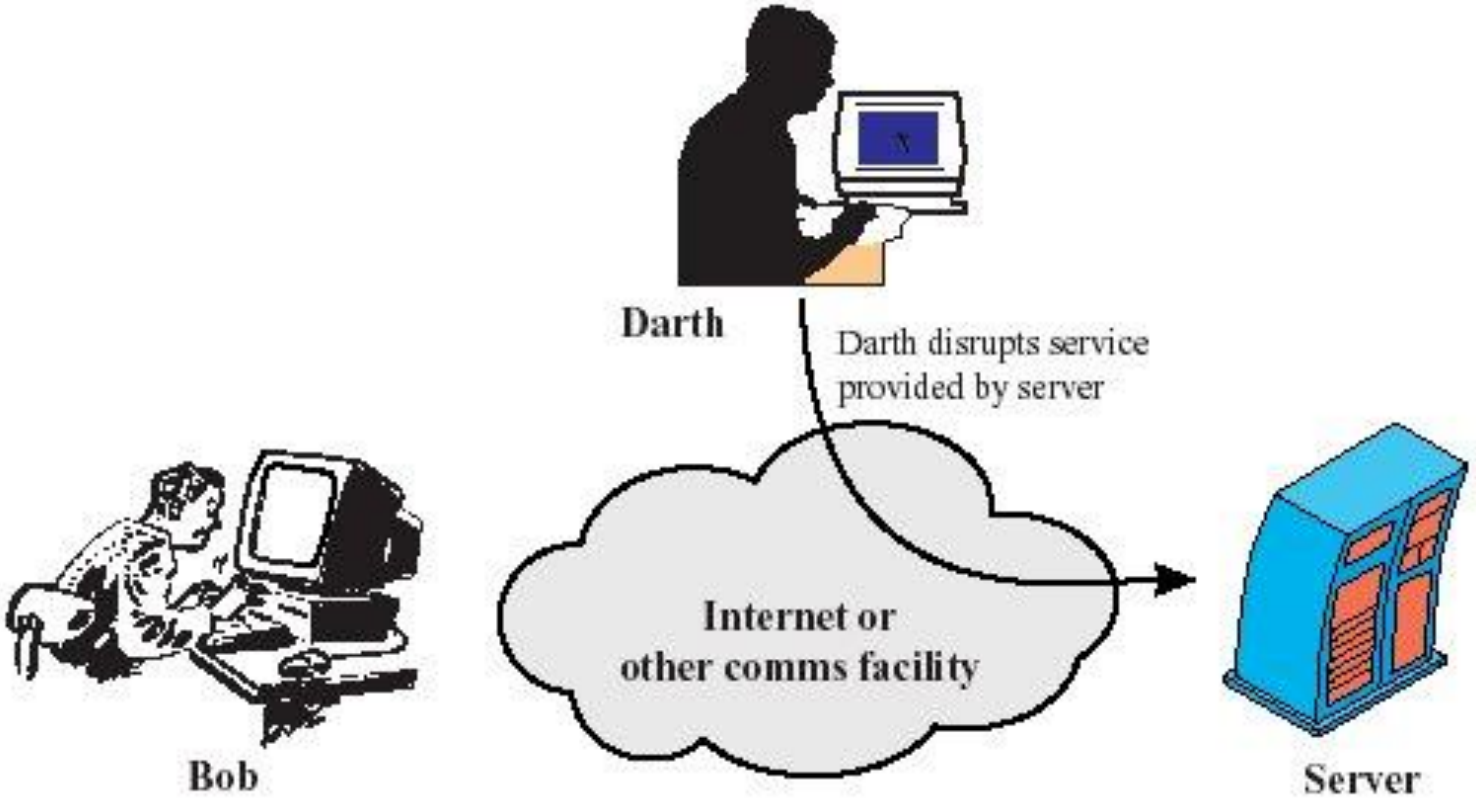
Description des attaques : Modification (main au milieu)

- Les attaques «Man in the Midlle » consistent pour un agresseur à s'insérer dans une communication en se positionnant en coupure entre un client et un serveur.
- L'agresseur peut alors :
  - Relayer les requêtes (écoute quasi passive)
  - Remplacer le serveur ou le client à tout moment (usurpation totale)



Déni de service ("DoS")

SYN Flooding: Elle consiste à émettre un flot ininterrompu de demandes de connexion sur un port TCP ouvert sans poursuivre les échanges, et de préférence en falsifiant l'adresse source.



Que faire

- Limiter les services
- Limiter l'accès à certaines machines
- Ne pas se connecter à Internet?

Mécanismes de défense

- **Chiffrement** : algorithme généralement basé sur des clefs et transformant les données. Sa sécurité est dépendante du niveau de sécurité des clefs.
- **Signature** numérique: données ajoutées pour vérifier l'intégrité ou l'origine des données.
- **Bourrage de trafic** : données ajoutées pour assurer la confidentialité, notamment au niveau du volume du trafic.
- **Notarisation** : utilisation d'un tiers de confiance pour assurer certains services de sécurité.
- **Contrôle d'accès** : vérifie les droits d'accès d'un acteur aux données. N'empêche pas l'exploitation d'une vulnérabilité.

Mécanismes de défense

- **Antivirus** : logiciel censé protéger ordinateur contre les logiciels néfastes. Ne protège pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire.
- **Le pare-feu** : un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent. Il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les communications autorisés ou interdits.
  - N'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système.
  - Ne protège pas contre une attaque venant du réseau intérieur (qui ne le traverse pas).

Mécanismes de défense

- **Détection d'intrusion** : repère les activités anormales ou suspectes sur le réseau surveillé. Ne détecte pas les accès incorrects mais autorisés par un utilisateur légitime. Mauvaise détection : taux de faux positifs, faux négatifs.
- **Journalisation** ("logs") : Enregistrement des activités de chaque acteurs. Permet de constater que des attaques ont eu lieu, de les analyser et potentiellement de faire en sorte qu'elles ne se reproduisent pas.
- **Analyse des vulnérabilité** ("security audit") : identification des points de vulnérabilité du système. Ne détecte pas les attaques ayant déjà eu lieu, ou lorsqu'elles auront lieu.

Mécanismes de défense

- **Contrôle du routage** : sécurisation des chemins (liens et équipements d'interconnexion).
- **Contrôle d'accès aux communications** : le moyen de communication n'est utilisé que par des acteurs autorisés. Par VPN ou tunnels.
- **Certification** : preuve d'un fait, d'un droit accordé.
- **Distribution de clefs** : distribution sécurisée des clefs entre les entités concernées.

Mécanismes de défense

Authentification :

- Authentifier un acteur peut se faire en utilisant une ou plusieurs de ses éléments.
  - Ce qu'il sait. Par ex. : votre mot de passe, la date anniversaire de votre grand-mère
  - Ce qu'il a. Par ex. : une carte à puce
  - Ce qu'il est. Par ex. : la biométrie (empreinte digitale, oculaire ou vocale)
- Dans le domaine des communications, on authentifie l'émetteur du message. Si l'on considère les (deux) extrémités d'une communication il faut effectuer un double authentification
  - Par ex. pour lutter contre le "phishing"
- L'authentification est nécessaire au bon fonctionnement des autres mécanismes.

Mécanismes de défense

La protection physique :

peut fournir une protection totale, mais qui peut être excessive. Par exemple isoler complètement son système est une solution qui peut être trop radicale.