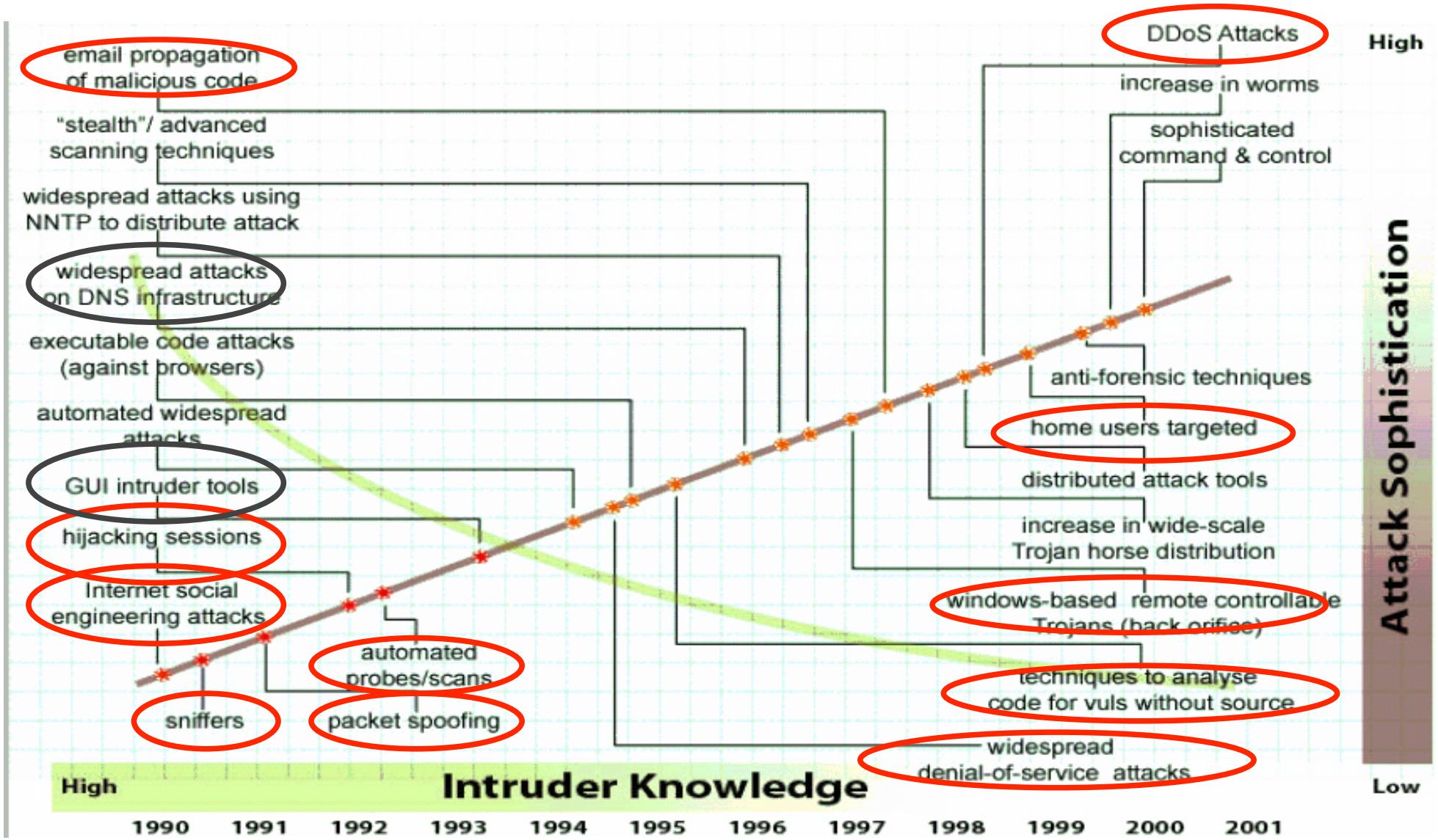
Normes et Sécurité
Chapitre 2 : Les attaques

sources:
lasecwww.epfl.ch
securit.free.fr
www.ssi.gouv.fr
…

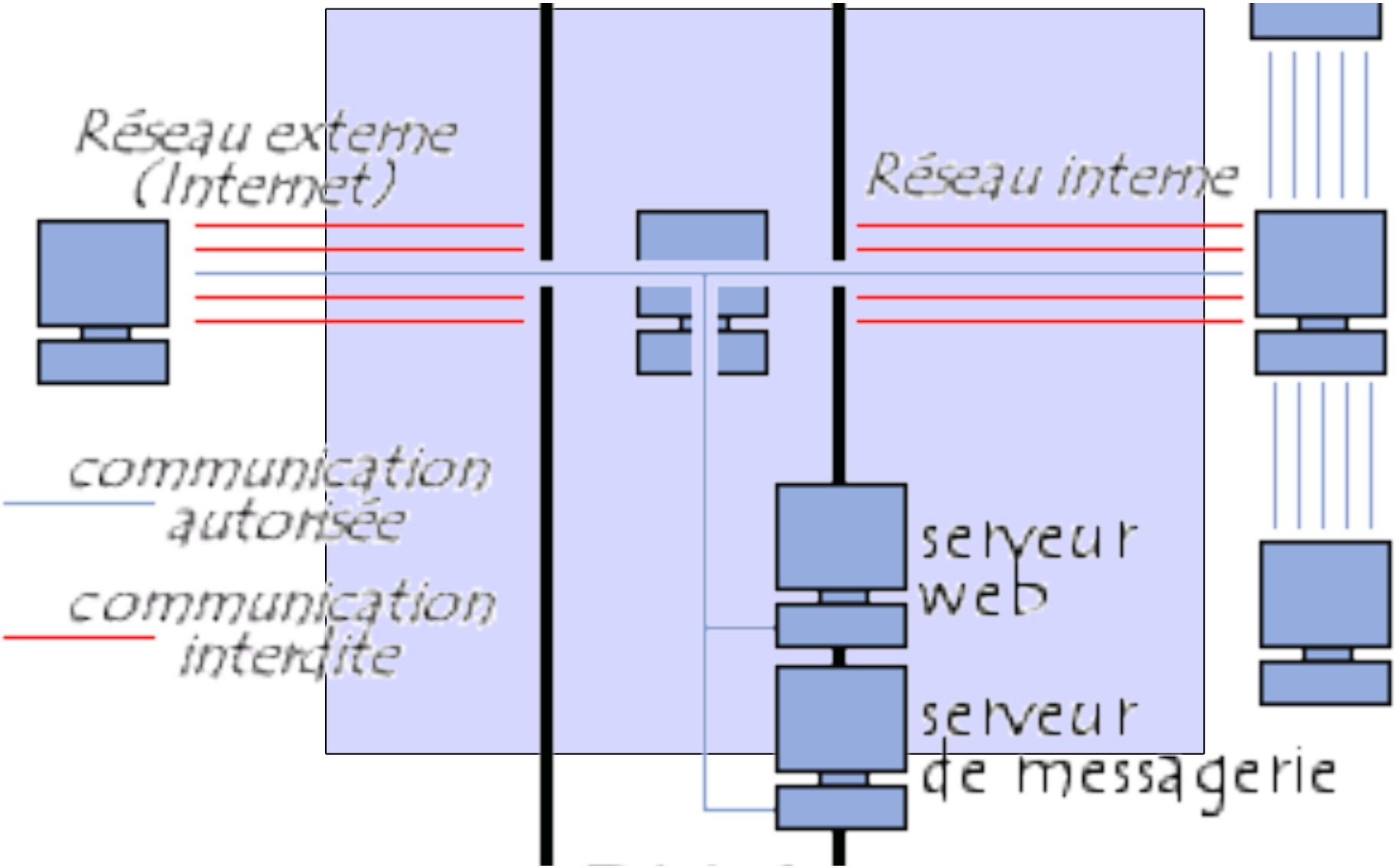
Introduction



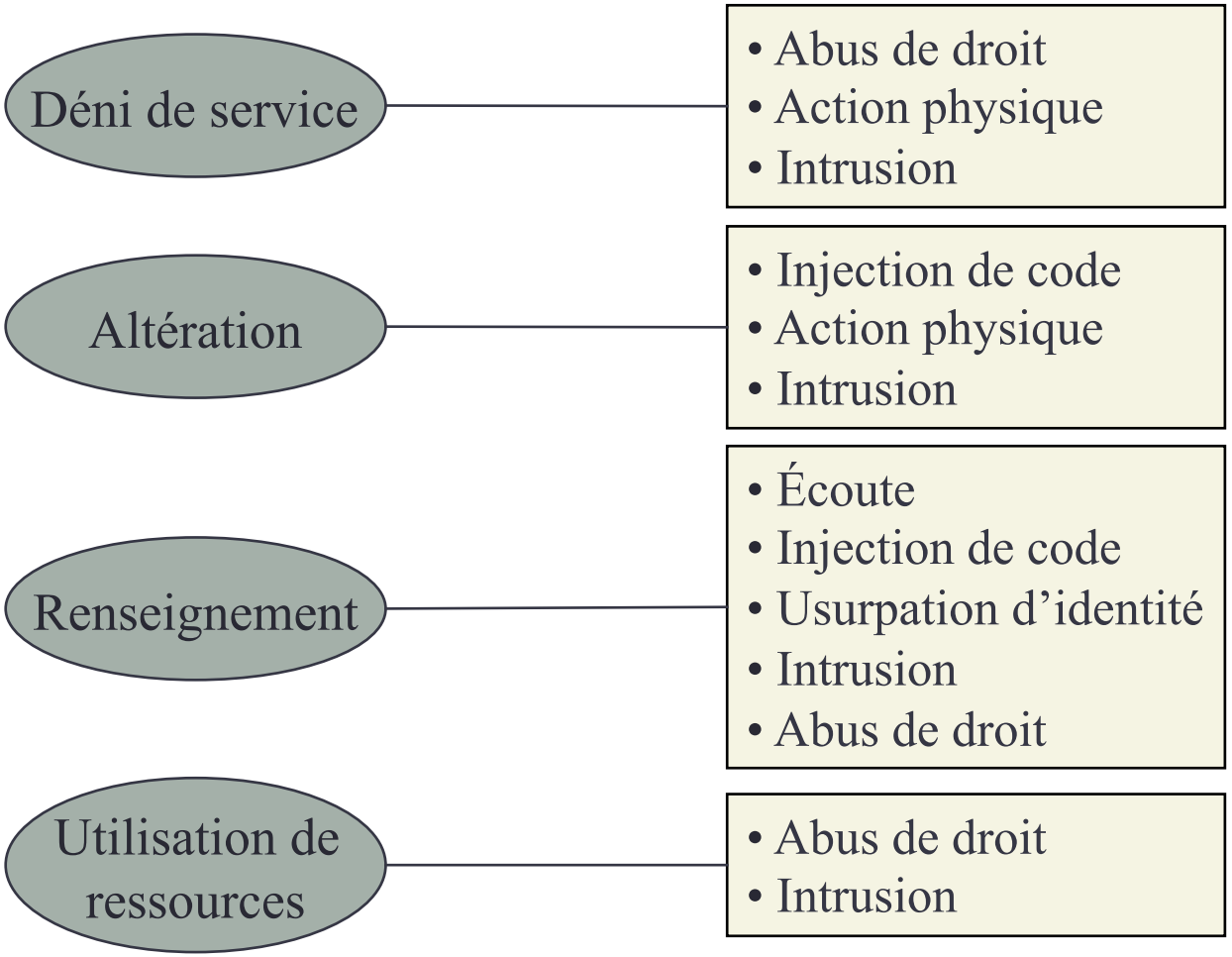
Introduction

- Vocabulaire :
  - Pare-feu (coupe-feu, garde-barrière ou firewall)
    - système pour protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet)
  - Bastion
    - Machines sécurisés du réseau accessibles de l'extérieur supportant les services comme la messagerie, HTTP, le FTP public, etc…
  - DMZ : zone démilitarisé
    - zone isolée hébergeant les applications accessible de l'extérieur
    - « zone tampon » entre le réseau à protéger et le réseau hostile.
  - IDS
    - Système de détection d'intrusion

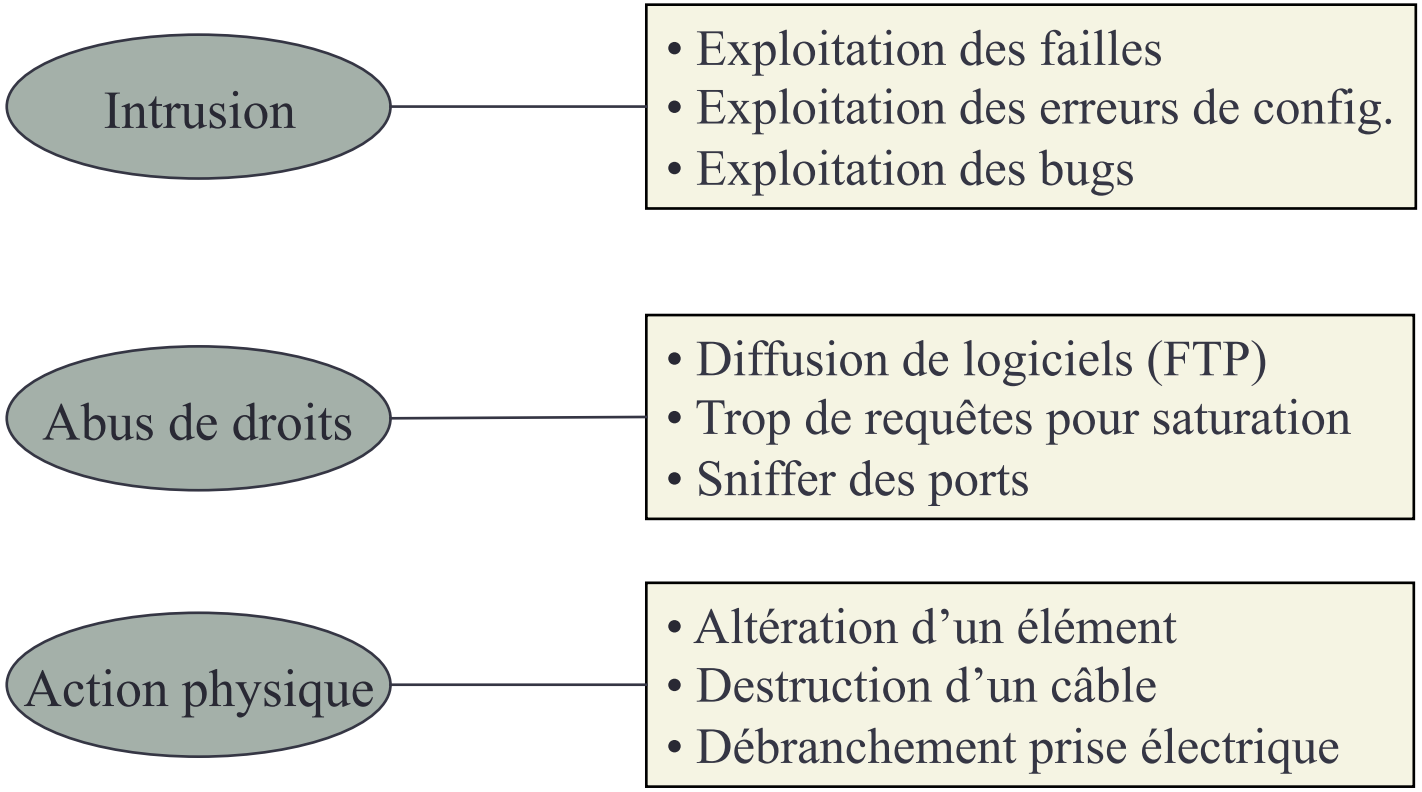
Introduction



Objectifs & méthodes



Méthodes & exemples



Plan

- I-Attaques sur l'information
- II-Attaques réseaux
  - faiblesses des protocoles réseaux
    - cartographie du réseaux, identification des systèmes, écoute du trafic
    - sauter le firewall, commutateur, DoS
  - faiblesses d'authentification(ARP, IP, mot de passe)
  - faiblesse d'implémentation, bogues (TCP syn, bogues IP/TCP, OS)
  - faiblesse de configuration (OS, mots de passe)
- III-Attaques indirectes
  - Mails
  - Virus, vers, cheval et autres animaux

Attaques sur l'information

- Collecte d'information (Footprinting)
  - l’attaquant doit se renseigner sur la cible
  - découvrir ou se trouvent les machines de la cible
  - Un première source d'information sont les registres de noms
    - enregistrement du domaine --> une adresse IP
    - bases de données whois de l'Internet
    - Les IP de l'Internet attribuées par cinq organismes
      - Pour l'Europe : RIPE (Réseaux IP Européens)
    - informations sont publiques :
      - les IP allouées, noms, adresses et numéro de téléphone des responsables

Attaques sur l'information

- Social Engineering
  - technique pour extirper des informations à des personnes
  - ne nécessite pas de logiciel
  - repose sur la force de persuasion
  - 4 grandes méthodes :
    - par téléphone
    - par lettre
    - par Internet
    - par contact direct

Attaques sur l'information : Social Engineering

- Par téléphone
  - technique la plus facile
  - Méthode : avoir le renseignement le plus rapidement possible
  - un bon attaquant
    - aura préparé son personnage et son discours
    - sera sûr de lui
    - sera très persuasif dans le timbre de sa voix
  - En cas de coup de fil d'une personne inconnue
    - → ne donnez aucun renseignement

Attaques sur l'information : Social Engineering

- Par lettre
  - lettre très professionnelle
  - papier à lettre avec :
    - logo,
    - adresse, téléphone, fax, email...
  - l’attaquant utilisera très certainement une boîte postale pour l'adresse de sa société fictive

Attaques sur l'information : Social Engineering

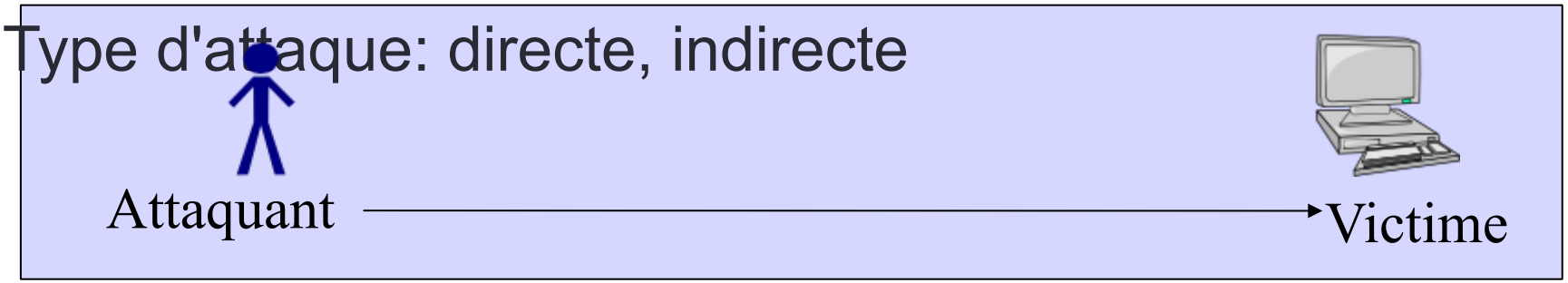
- Par internet
  - idem au téléphone
  - l'attaquant se fera passer pour un administrateur système, un responsable informatique ou un ingénieur système
- Par contact direct
  - plus dur à faire
  - le paraître compte beaucoup :
    - costard / cravate, attaché-case , agenda rempli, documents divers, carte de visite, badge...
  - risques important pour l'attaquant
    - il est déterminé à obtenir les renseignements souhaités
    - → il sera donc très persuasif et préparé

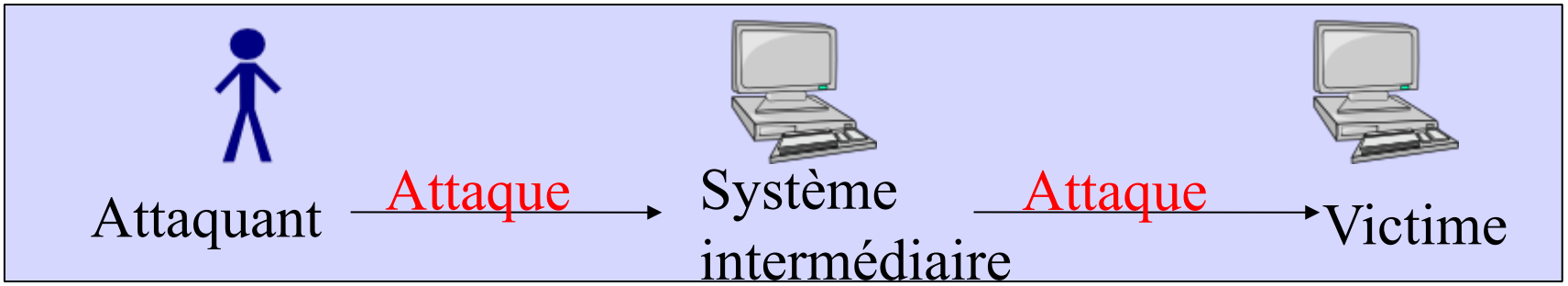
Plan

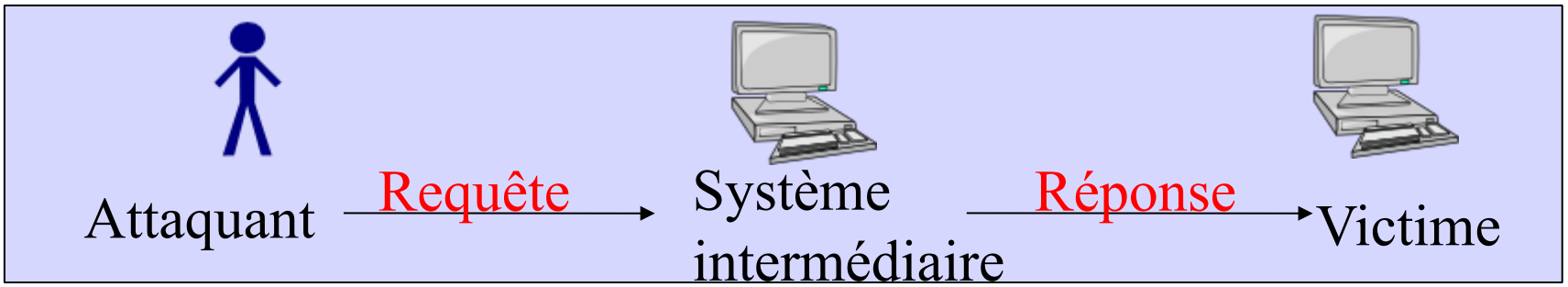
- I-Attaques sur l'information
- II-Attaques réseaux
  - faiblesses des protocoles réseaux
    - cartographie du réseaux, identification des systèmes, écoute du trafic
    - sauter le firewall, commutateur, DoS
  - faiblesses d'authentification(ARP, IP, mot de passe)
  - faiblesse d'implémentation, bogues (TCP syn, bogues IP/TCP, OS)
  - faiblesse de configuration (OS, mots de passe)
- III-Attaques indirectes
  - Mails
  - Virus, vers, cheval et autres animaux

Attaques réseaux

- Type d'attaque: directe, indirecte

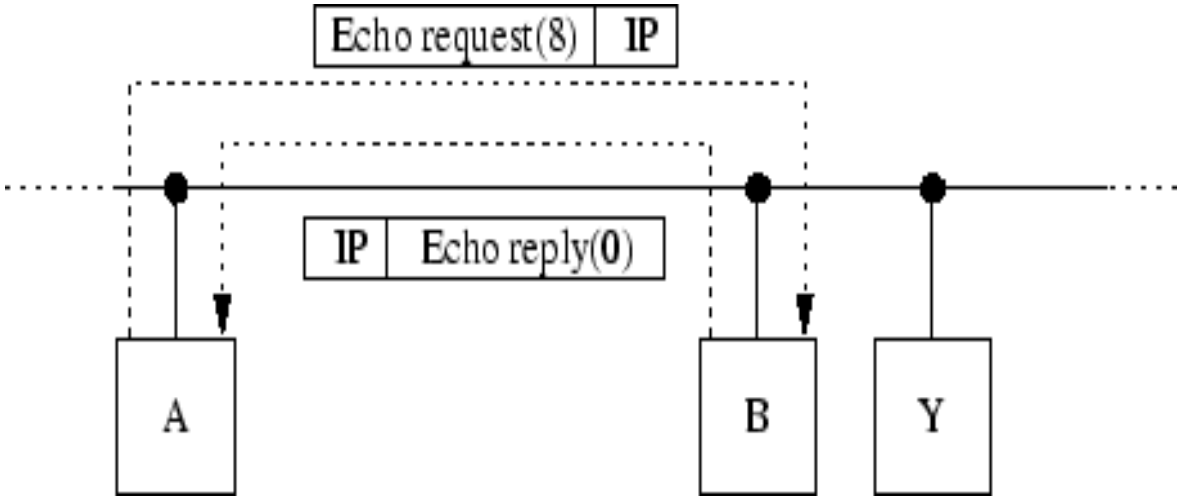






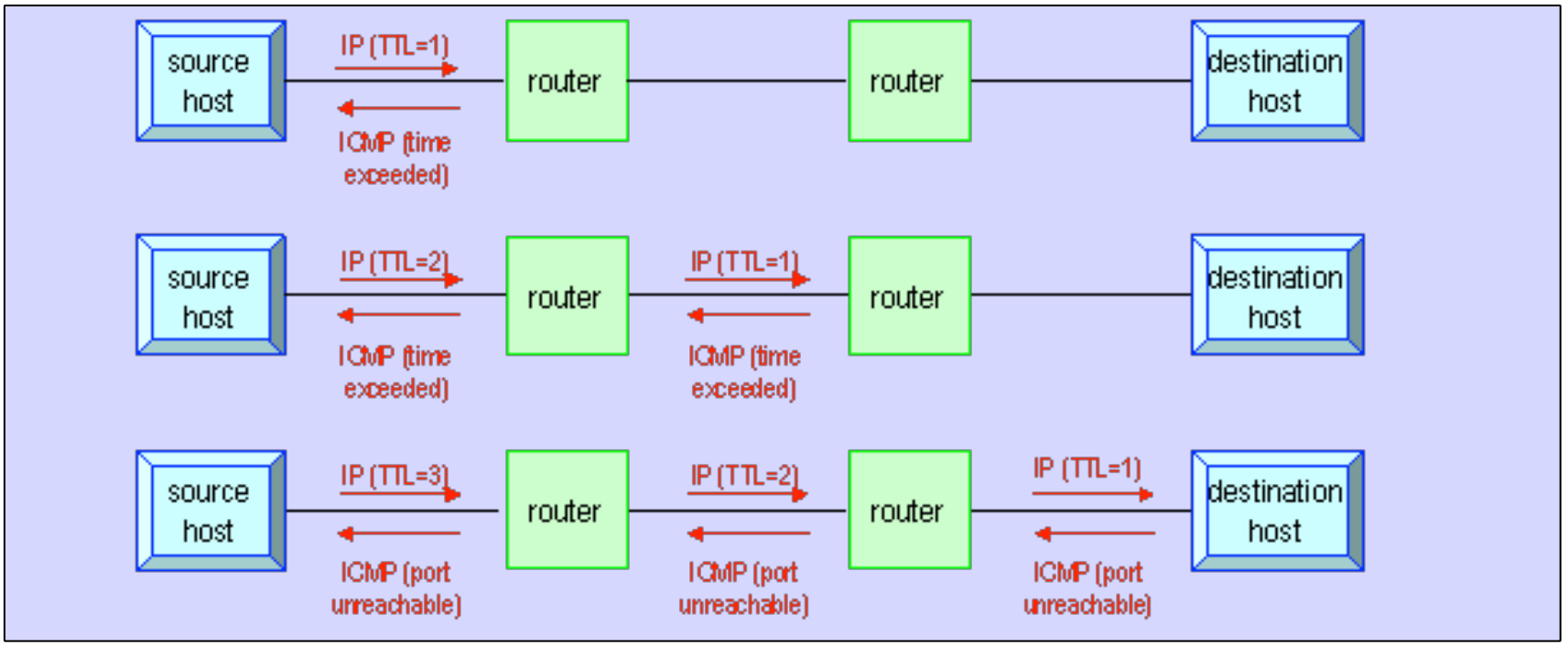
Attaques réseaux : Trouver une cible

- Ping : une machine répond si elle est active
- Protocole ICMP
  - Internet Control Message Protocol
  - RFC 950
- Généralement bloqué
- Permet de connaître les machines d'un réseau



Repérer la topologie du réseau

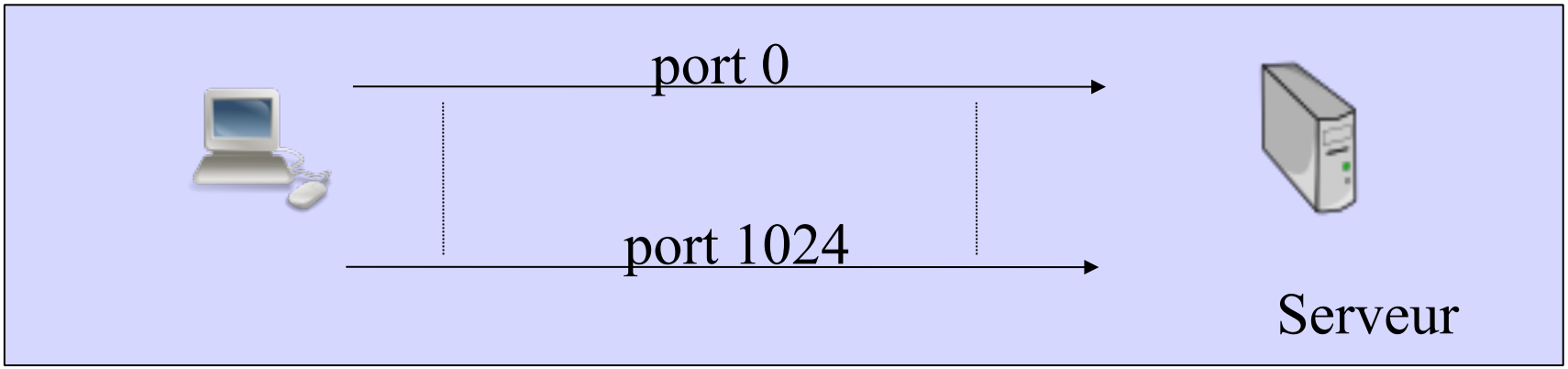
- Outil : traceroute
  - Première étape d'une future attaque d'un réseaux
  - Bloquer par les firewall
  - Cartographie du réseau



http://candle.ctit.utwente.nl/wp5/tel-sys/exercises/traceroute/traceroute.html

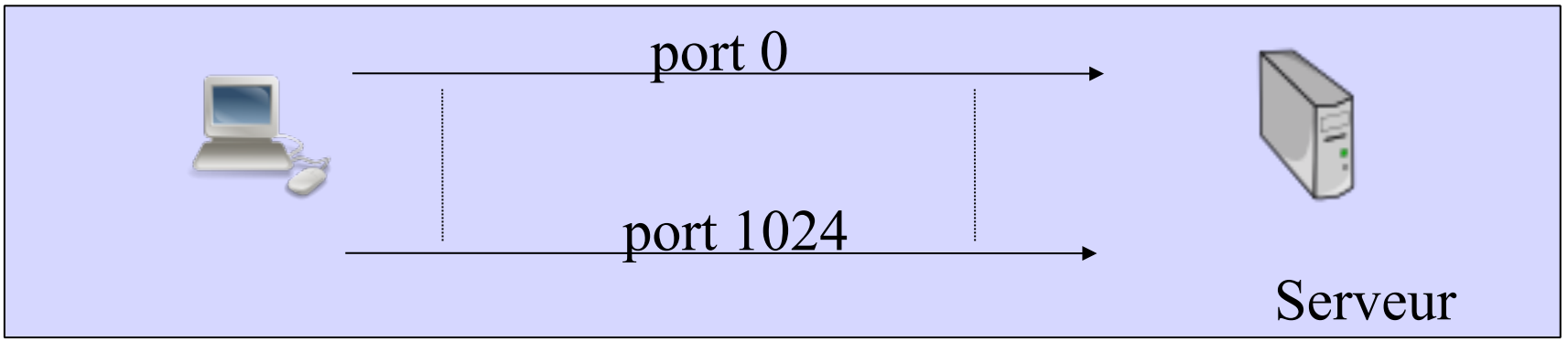
Identification des systèmes du réseau

- Nom : Scanning
  - Identifié un système : type d'OS, services TCP/UDP
  - Dresser les moyens de pénétration
  - Différent type de scan : cf doc
- Outils : nmap (généraliste), sscan (spécialisé)



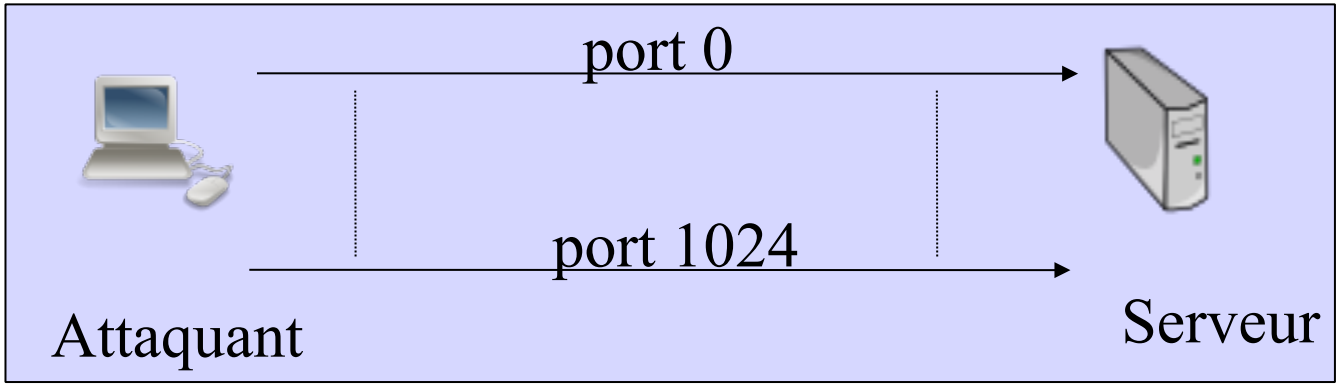
Identification des systèmes du réseau

- Nom : Scanning
- Différent type de balayage
  - scan ouvert : connexion TCP complète
  - scan semi-ouvert : semi-connexion avec drapeau SYN
  - scan furtif : semi-connexion avec drapeau SYN|ACK
  - scan par contrôle d'erreur : ICMP echo
  - autres types de scan : UDP...



Identification des systèmes du réseau

- [root@nowhere.net /root]# nmap 192.168.1.1
- Starting nmap V. 2.54BETA31 (www.insecure.org/nmap/)
- Interesting ports on (192.168.1.1) :
- (The 1544 ports scanned but not shown below are in state : closed)
- Port State Service
  - 21/tcp open ftp
  - 53/tcp open domain
  - 80/tcp open http
  - 110/tcp open pop-3
  - 111/tcp open sunrpc
  - 113/tcp open auth
  - 631/tcp open cups
  - 845/tcp open unknown
  - 901/tcp open samba-swat
  - 10000/tcp open snet-sensor-mgmt



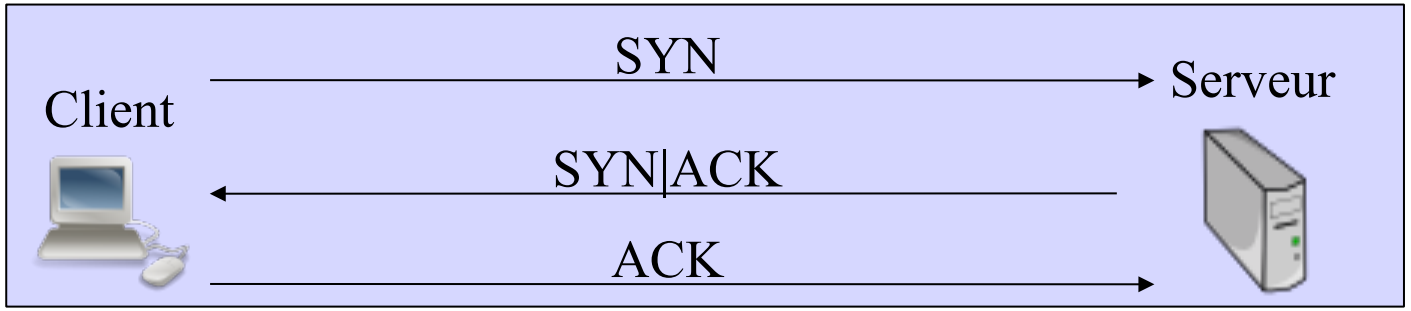
Identification des systèmes du réseau

- Scan TCP ouvert
  - Etablissement d'une connexion TCP, puis fermeture
  - Facile à détecter
- SYN : synchroniser les numéros de séquence
- ACK : le numéro d'acquittement du paquet est significatif
- RST : réinitialiser la connexion

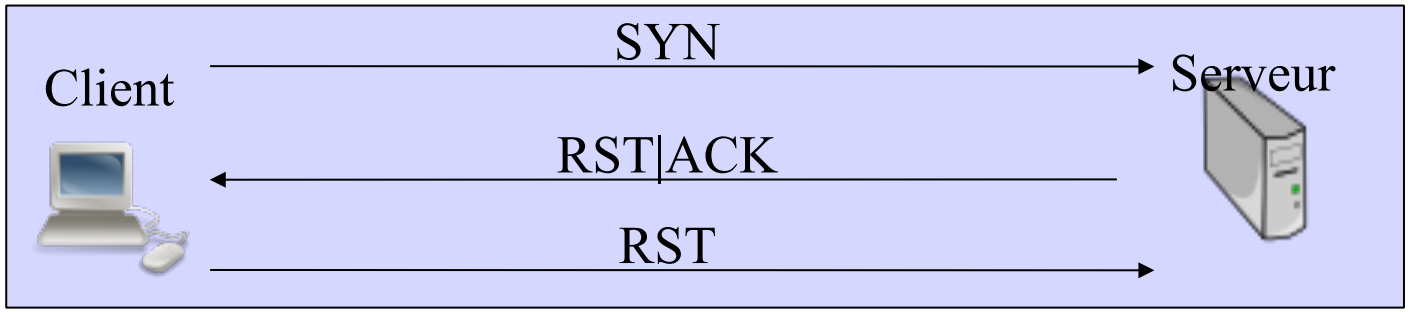
Connexion OK

=

le service existe



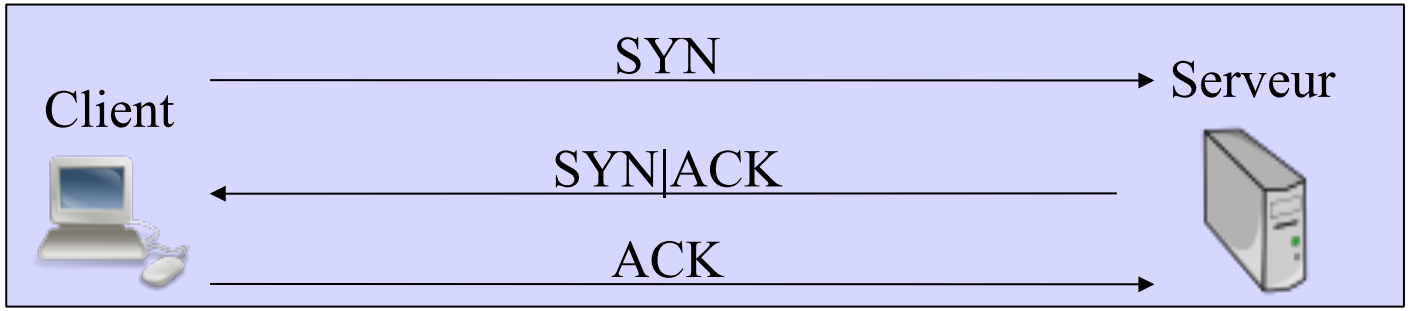
Connexion $\overline{\text{OK}}$



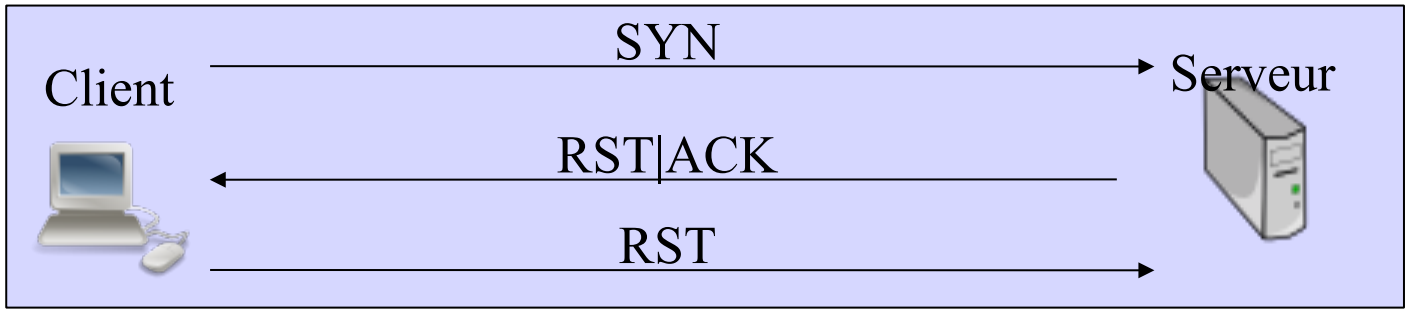
Identification des systèmes du réseau

- Scan TCP ouvert
  - Avantages :
    - rapide, précis, ne requière pas de privilèges particuliers
  - Inconvénients :
    - facilement détectable et enregistrable [NdT : logged]

Connexion OK
=
le service existe



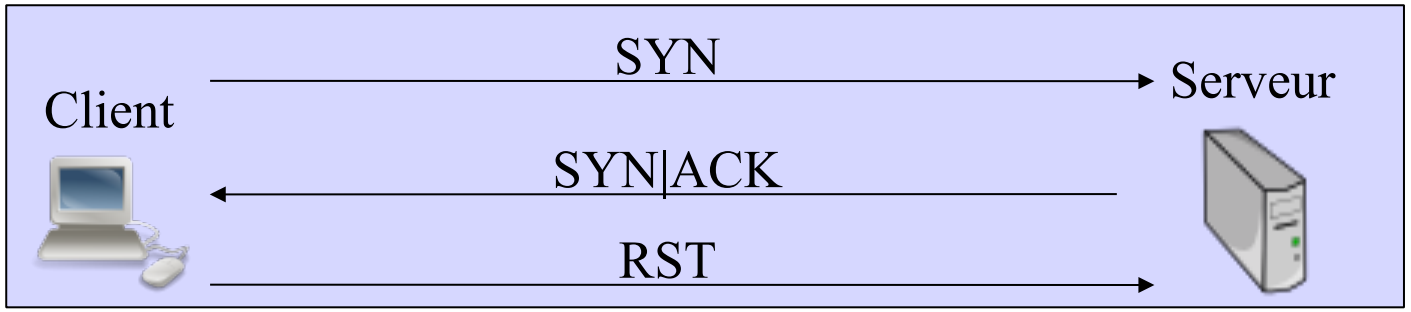
Connexion $\overline{\text{OK}}$



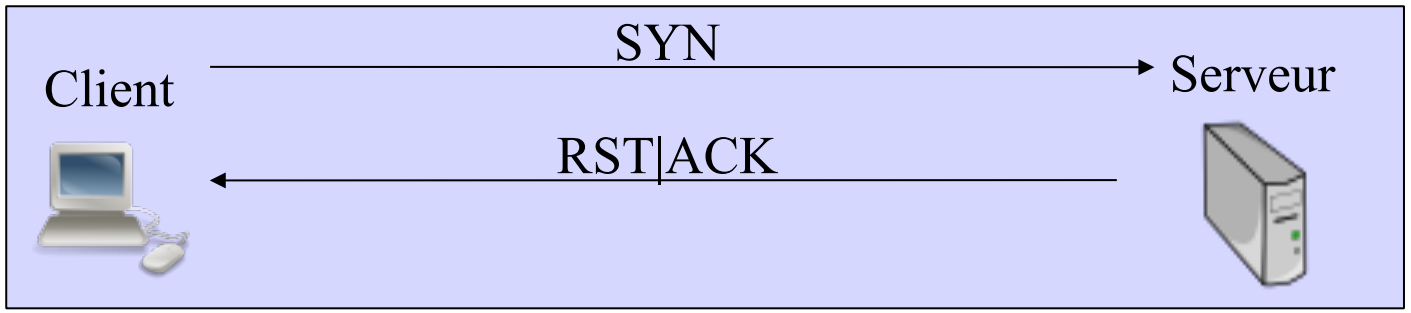
Identification des systèmes du réseau

- Scan TCP semi-ouvert :
  - Connextion TCP ne terminant pas la connexion
  - Envoie de RST au lieu de ACK (RST : réinitialiser la connexion)

Connexion OK



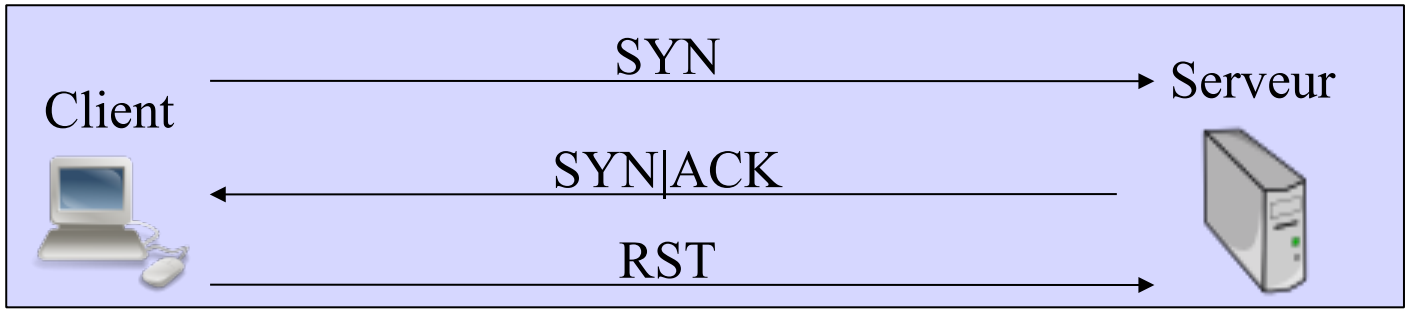
Connexion $\overline{\text{OK}}$



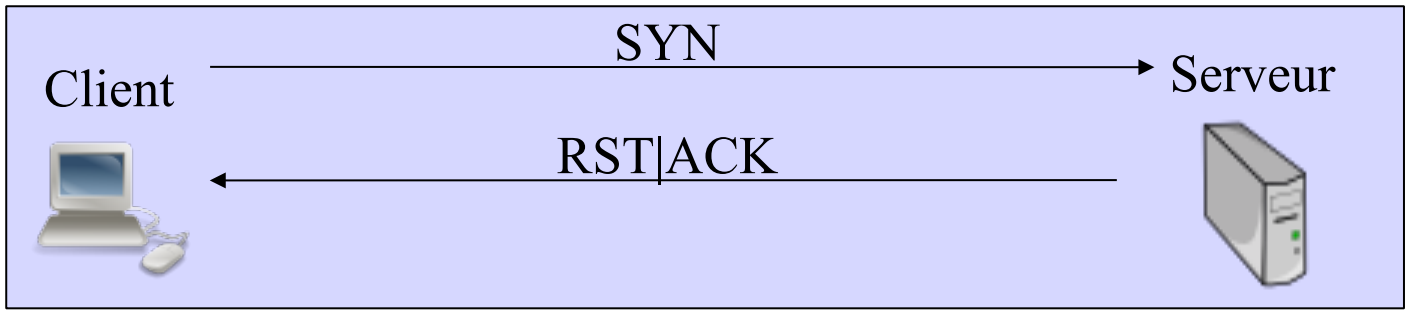
Identification des systèmes du réseau

- Scan TCP semi-ouvert :
  - Avantages :
    - rapide, fiable, évite les IDS primaires, évite l'accord TCP en trois étapes
  - Inconvénients :
    - requière le privilège root, règles empêchant beaucoup d'essais de scan SYN

Connexion OK



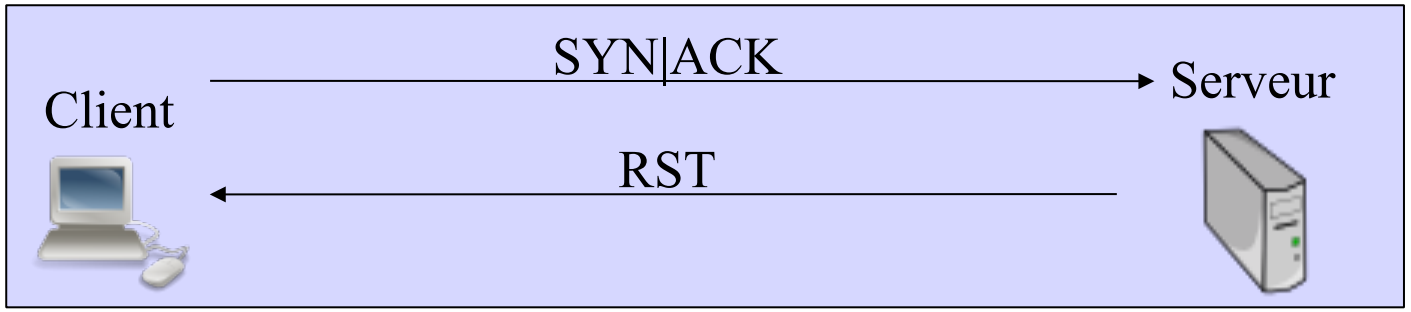
Connexion $\overline{\text{OK}}$



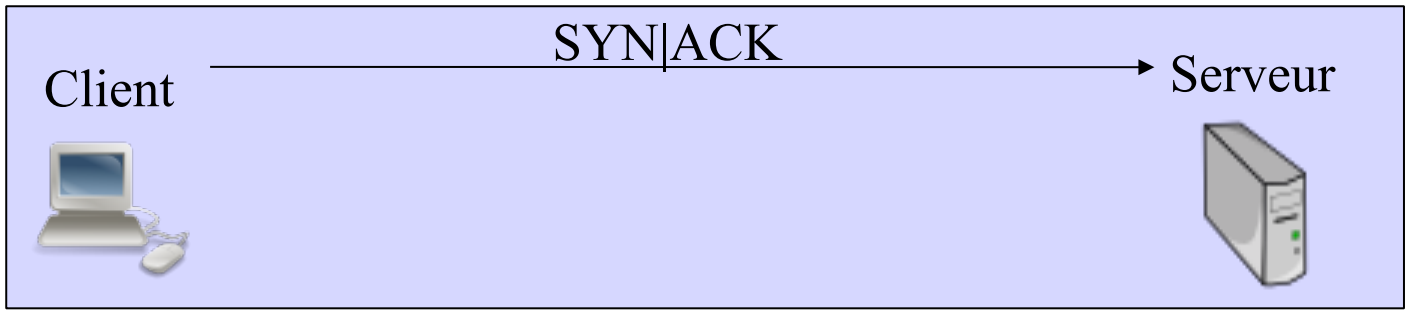
Identification des systèmes du réseau

- Scan TCP furtif
  - Différent type utilisant les flags ACK, FIN, RST, NULL...
  - Difficilement détectable
  - Moins précis

Connexion OK



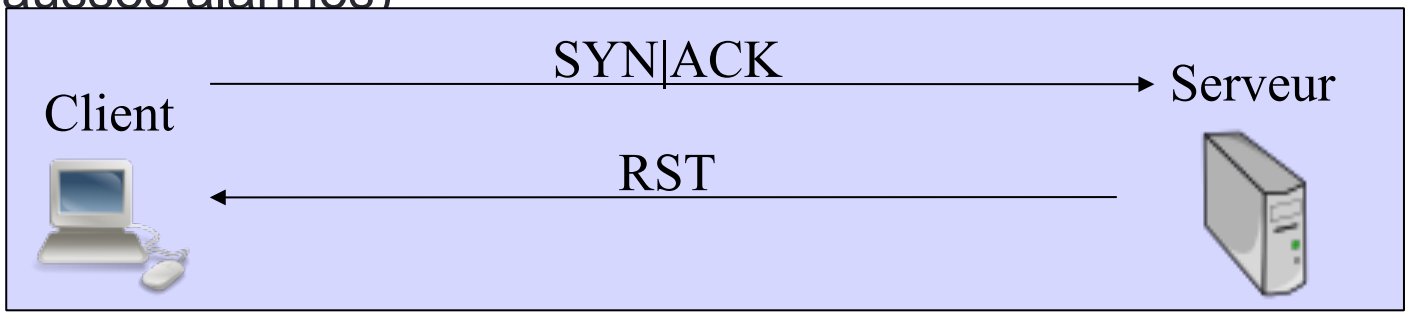
Connexion $\overline{\text{OK}}$



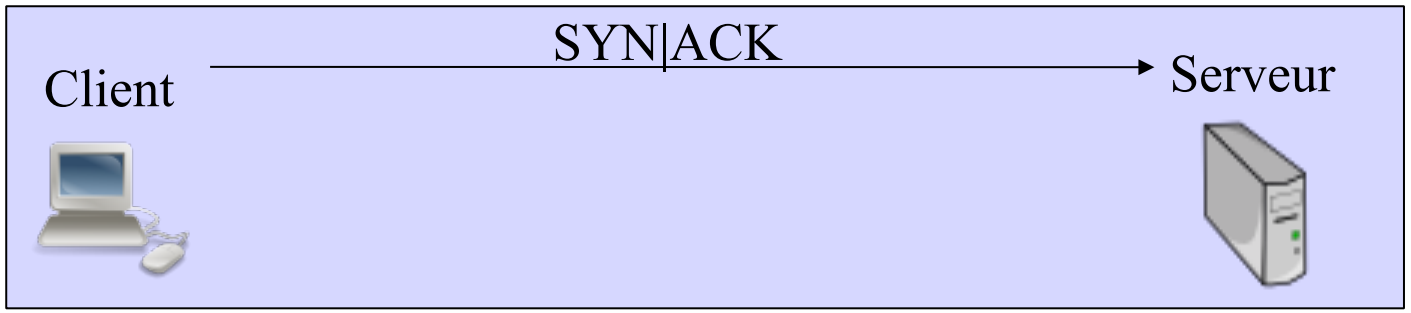
Identification des systèmes du réseau

- Scan TCP furtif
  - Avantages :
    - rapide, évite les parefeux/IDS basiques, évite l'accord TCP en trois étapes
  - Inconvénients :
    - moins solide (fausses alarmes)

Connexion OK



Connexion $\overline{\text{OK}}$

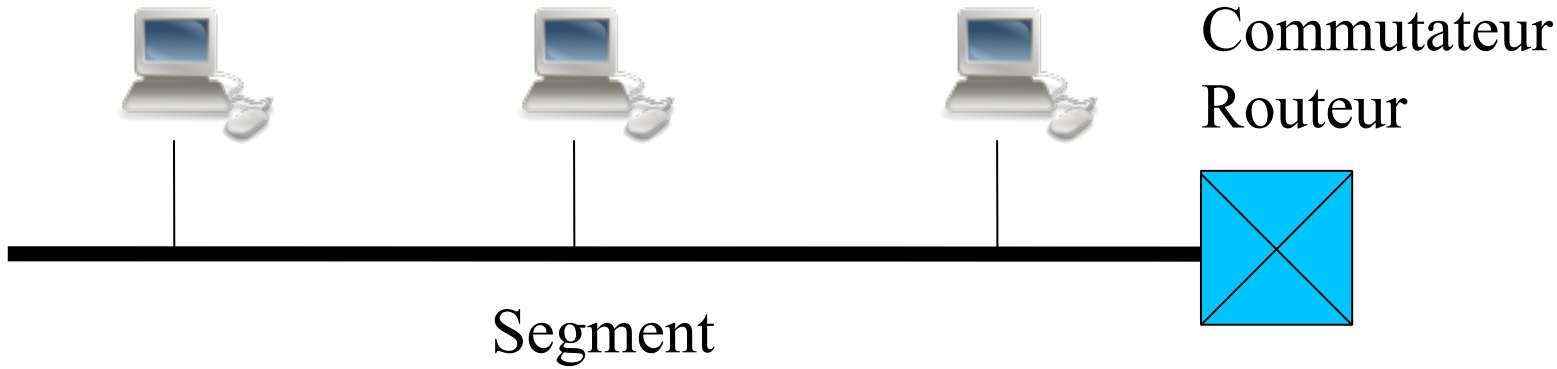


Identification des systèmes du réseau

- Scan en mode distribué
  - Utiliser N machines, centralisé les informations, partage des info
  - Script kiddies
- il existe d'autre type de scan
  - Exemple :
    - Découvrir si une machine est un firewall
    - Découvrir le type d'OS
  - cf nmap

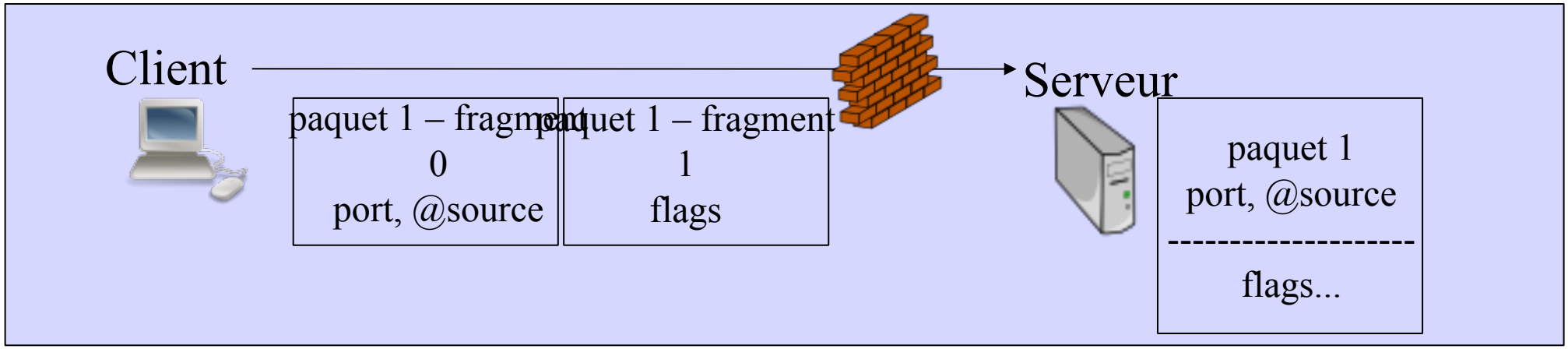
Écouter le trafic réseau

- Nom : Sniffing
  - But
    - Généralement utiliser pour capturer les mots de passe
  - Principe
    - Intercepter les données passant sur un segment du réseau
    - Besoin d'un accès administrateur



Attaques réseaux : faiblesse des protocole

- Exemple : fragmentation des paquets IP
  - But : attaque pour passer les firewalls
  - Attaque : Tiny fragments
    - Fragmenter sur deux paquets une demande de connexion TCP
      - 1er paquet = les 8 octets TCP (port source + destination + # de synchronisation)
      - 2ème paquet = le reste avec les flag SYN = 1 et ACK = 0
    - Règle de filtrage appliquée sur le premier paquet
    - Actuellement : les firewalls regardent tous les fragments



Attaques réseaux : Déni de Service

- Attaque par déni de service (DoS)
  - But : rendre indisponible un service, un système, un réseau
  - Utilise :
    - Une faiblesse d'implémentation / de protocole
    - Un bogue
  - Première attaque en 1998 et 2000
  - Principe général : Attaque par inondation
    - Inonder le réseau/une machine avec des paquets --> saturation
    - ou envoyer des attaques sur les faiblesses OS / protocoles
    - But :
      - occuper toute la bande passante,
      - la victime ne peut plus fonctionner correctement

Attaques réseaux : Déni de Service

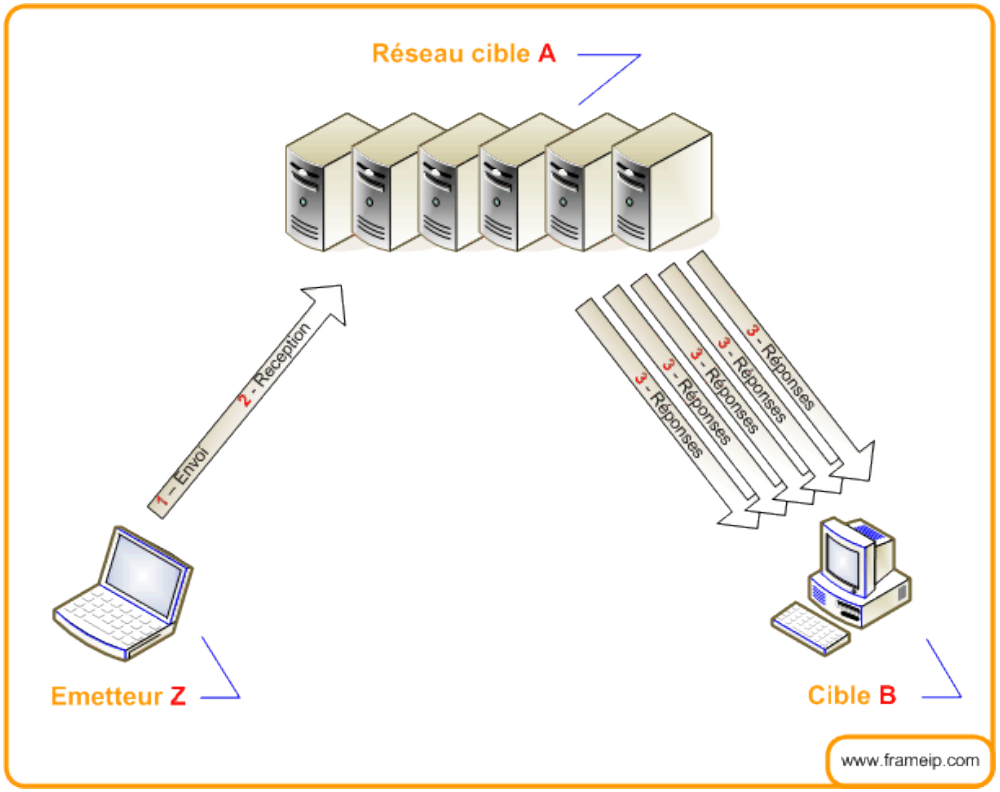
- Exemple simple : ping flooding
  - Consiste à envoyer un flux maximal de ping vers une cible
  - Nécessité d’avoir une plus grande bande passante que la cible
  - Conséquences :
    - Ralentissement système
    - Blocage système
    - Crash système
  - Comment s'en protéger ?
    - Utilisation d'un firewall

Attaques réseaux : Déni de Service

- Exemple 2 : Attaque par smurf-and-fraggle
  - Principe
    - Idem au flooding
    - Utilisation d'un réseau tiers
    - Ping utilisant des adresses de diffusion avec une fausse adresse source
    - Utilisation d'une faiblesse de configuration des routeurs
      - Le pare-feu ne devrait pas accepter la requête ping
      - Adresses de diffusion doivent être filtrer sur le pare-feu

Attaques réseaux : Déni de Service

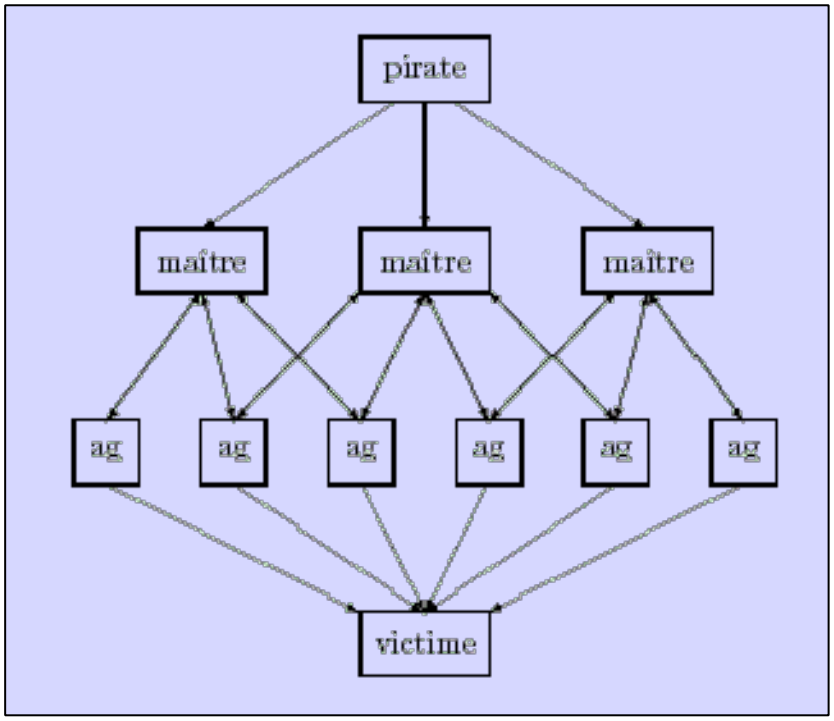
- Exemple 2 : Attaque par smurf-and-fraggle
  - smurf --> TCP ; fraggle --> UDP



http://www.frameip.com/smurf/

Attaques réseaux : Déni de Service Distribué

- Attaque par déni de service distribué (DDoS)
  - Utilisation de N machines esclaves pour saturer la victime
  - Hiérarchie de machines
  - Exemple
    - TFN (Tribe Flood Network), Stacheidrath (TFN + cryptage)
    - Trinoo
    - TFN2K (TFN + port au hasard)

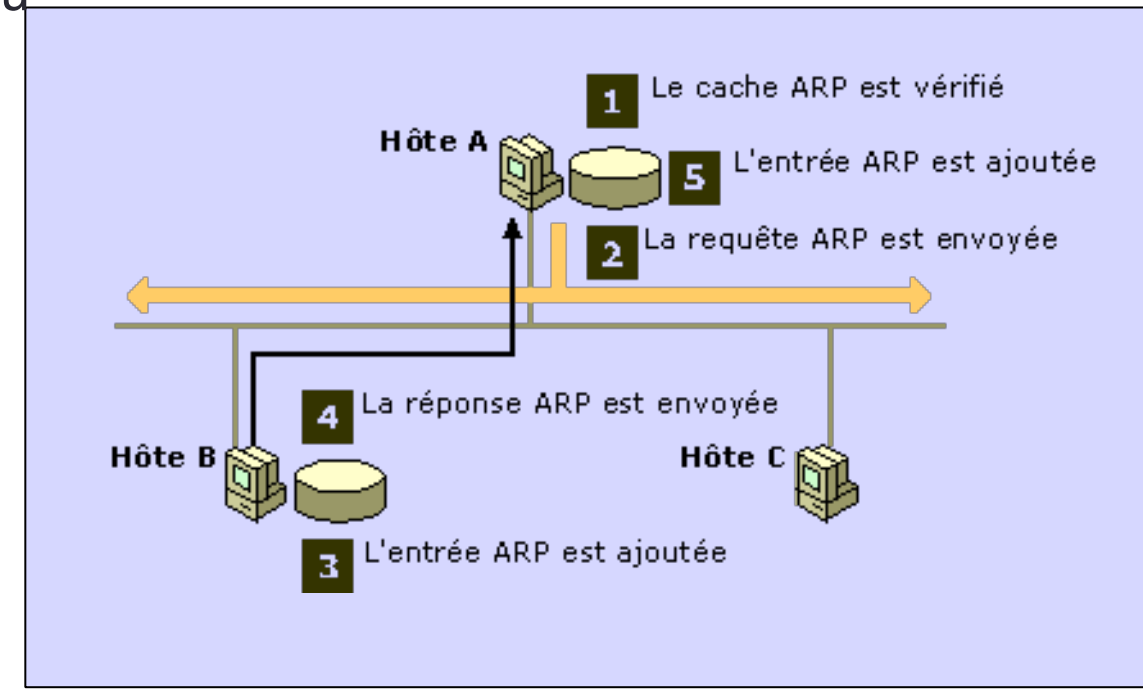


Attaques réseaux : Faiblesse d'authentification

- Mécanisme d'authentification dans les protocoles
  - La source est-elle bien l'auteur de l'information ?
- Des protocoles n'ont pas de mécanisme d'authentification fiable
- Exemple de d'attaques :
  - Spoofing : ARP, IP, DNS
    - Technique consistant à utiliser l'adresse d'une machine afin d'en usurper l'identité.
    - Permet de récupérer l'accès à des informations en se faisant passer pour la machine dont on « spoofe »l'adresse IP
  - Principe de « man-in-the-middle »
    - vol de session TCP (session hijacking)

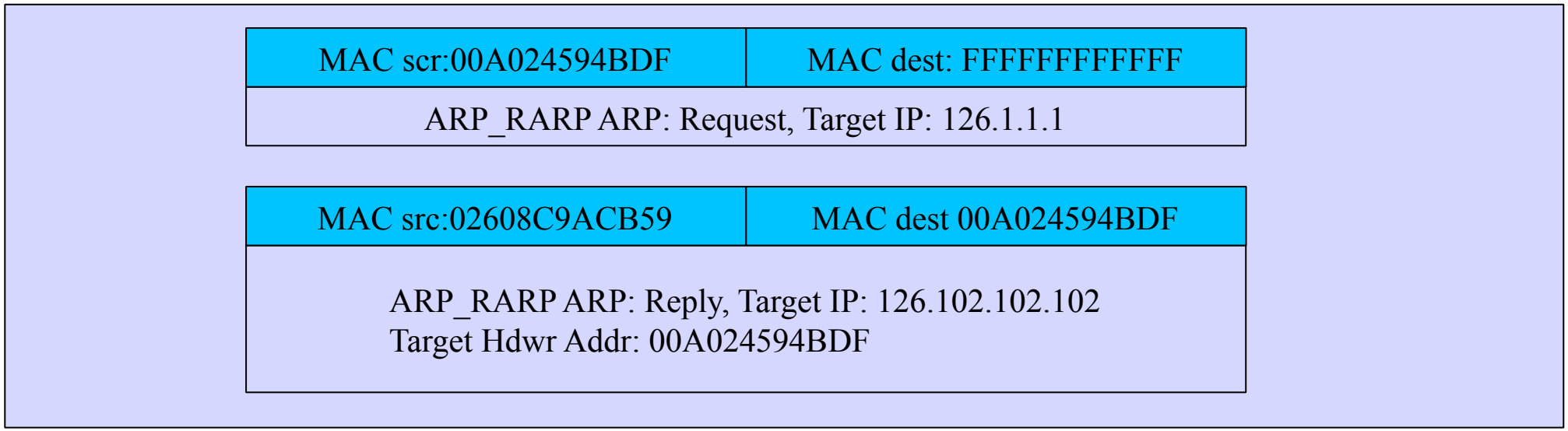
Attaques réseaux : Faiblesse d'authentification

- Attaque ARP spoofing
  - Protocole ARP (Adress Resolution Protocol)
    - résolution adresse MAC (niveau 2 du modèle OSI)
    - Exemple d'adresse MAC : 00-AA-00-3F-89-4A
    - Chaque entité maintient une table de correspondance entre IP et MAC



Attaques réseaux : Faiblesse d'authentification

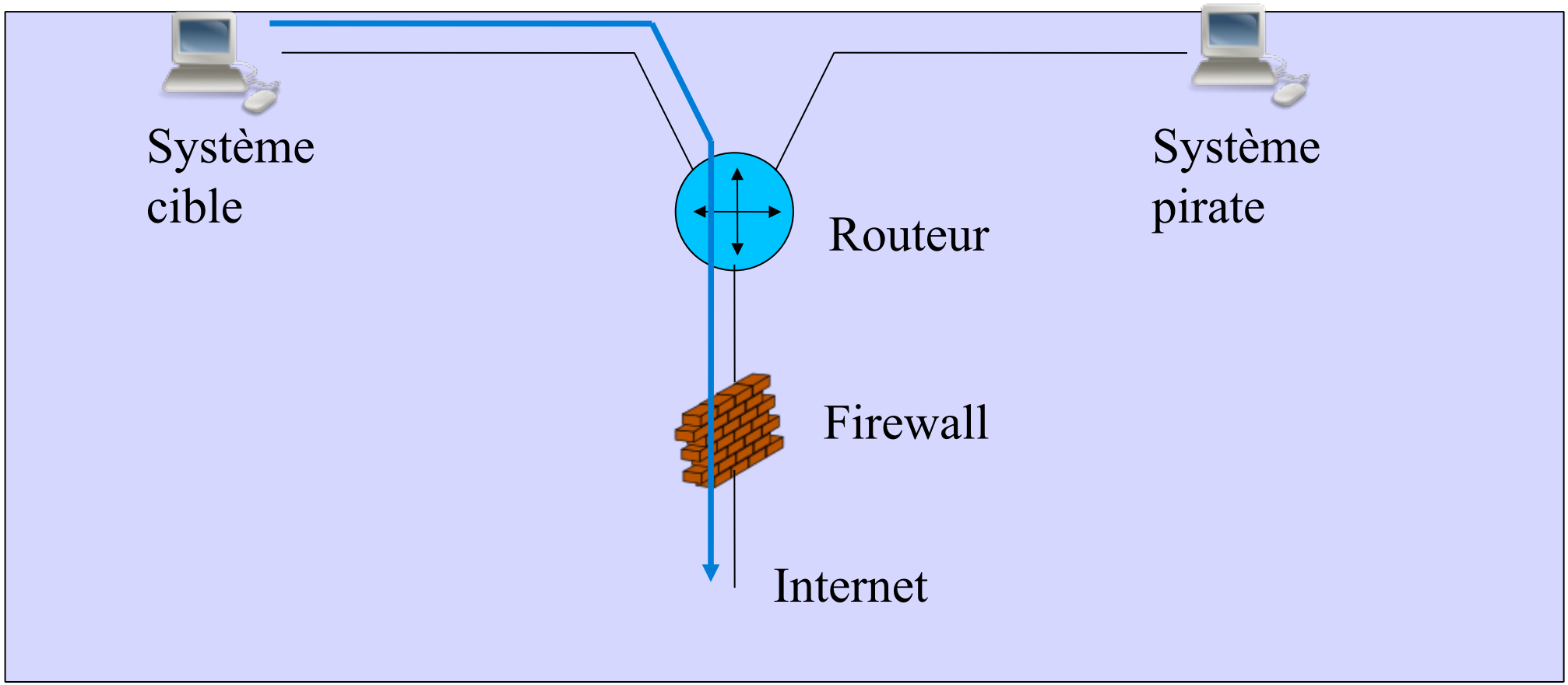
- Attaque ARP spoofing
  - S'appuie sur le protocole ARP (Adress Resolution Protocol)
  - Requête ARP



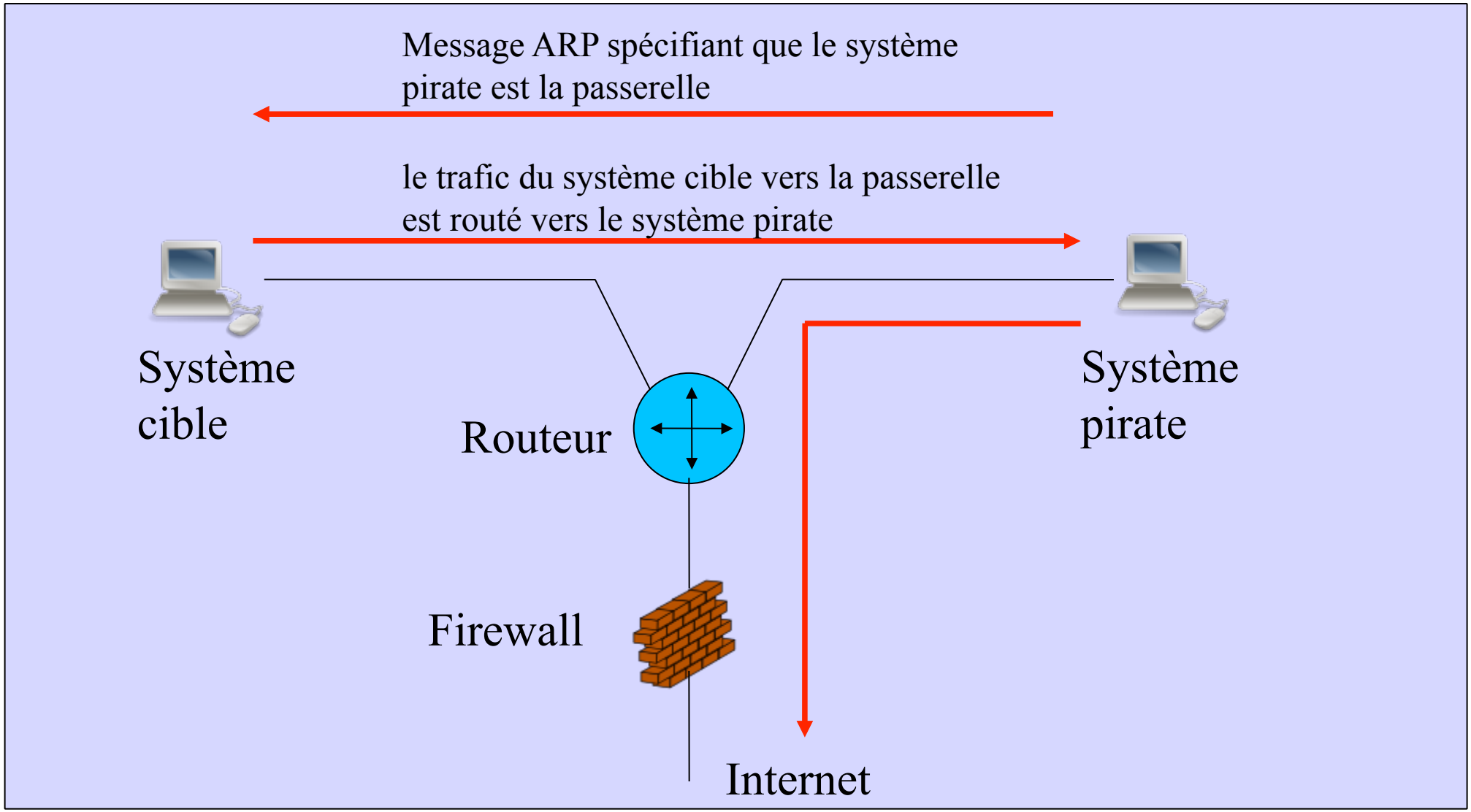
- Principe
  - répondre à la place de la cible avec son adresse IP
    - cible = une passerelle, une machine

Attaques réseaux : Faiblesse d'authentification

- Dérouter le trafic vers soit en se faisant passer pour la passerelle



Attaques réseaux : Faiblesse d'authentification

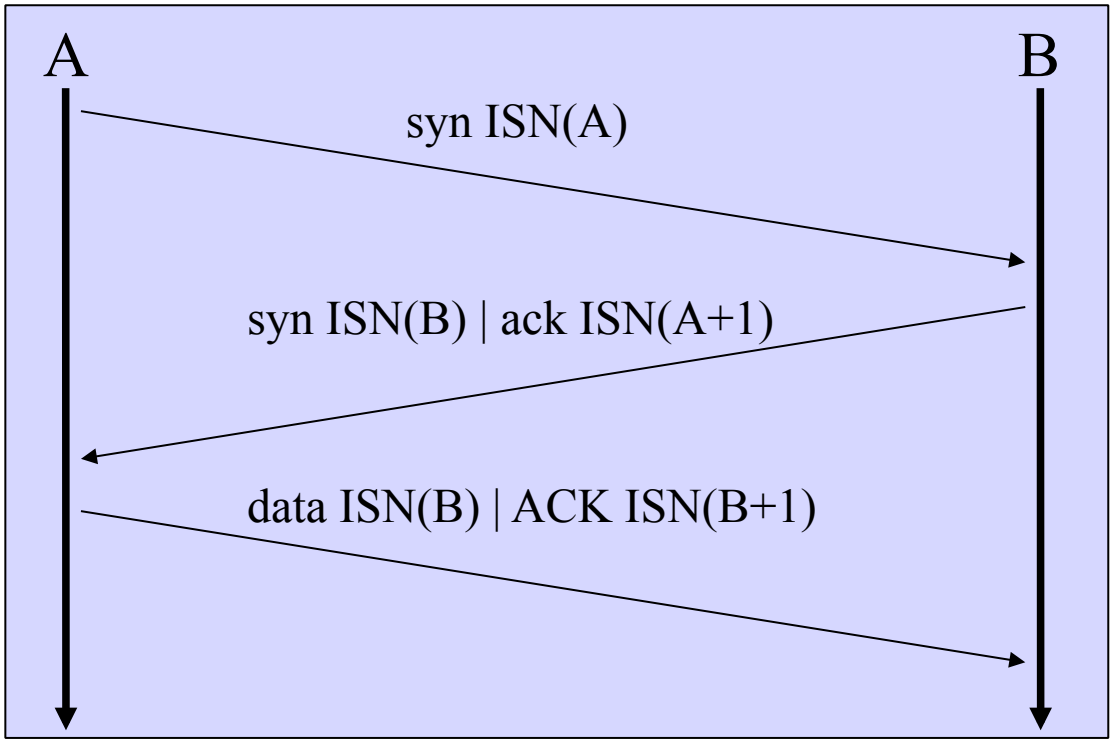


Attaques réseaux : Faiblesse d'authentification

- Attaque IP spoofing
  - Dans certains cas, l'adresse source IP est utilisée pour autoriser une communication
    - Certains programmes (rlogin, rsh) peuvent autoriser certaines sources à se connecter sans authentification.
    - Il est facile de forger l'adresse source d'un paquet IP et d'usurper la confiance faite à cette source
    - la réponse à un message forgé est envoyée à l'adresse usurpée

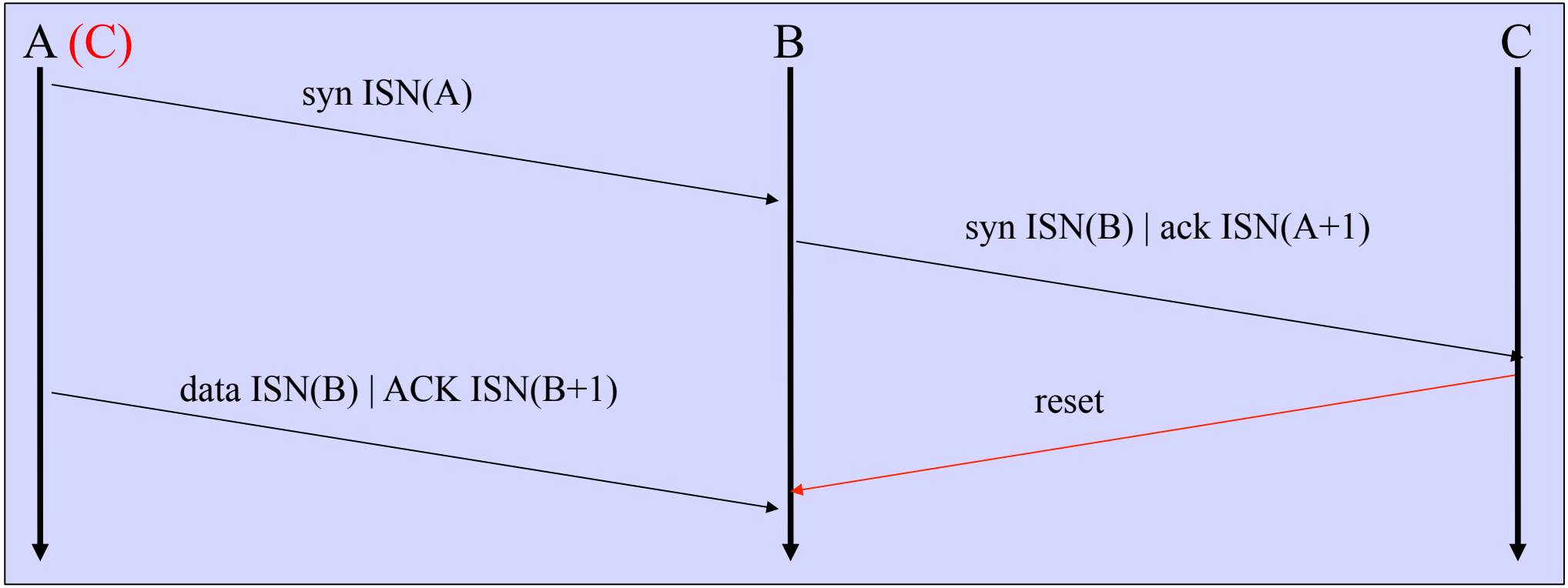
Attaques réseaux : Faiblesse d'authentification

- Les applications à pirater (rlogin, rsh, ..)
  - TCP utilise des numéros de séquence pour suivre les données envoyées et reçues
  - un numéro de séquence initial aléatoire (ISN) est choisi pour chaque nouvelle connexion



Attaques réseaux : Faiblesse d'authentification

- Attaque
  - A envoie ses paquets avec une adresse source C
  - Il doit deviner l'ISN que B va proposer à C
  - C, qui n'a rien demandé à personne, envoie un reset à B
  - Le pirate doit empêcher C de répondre

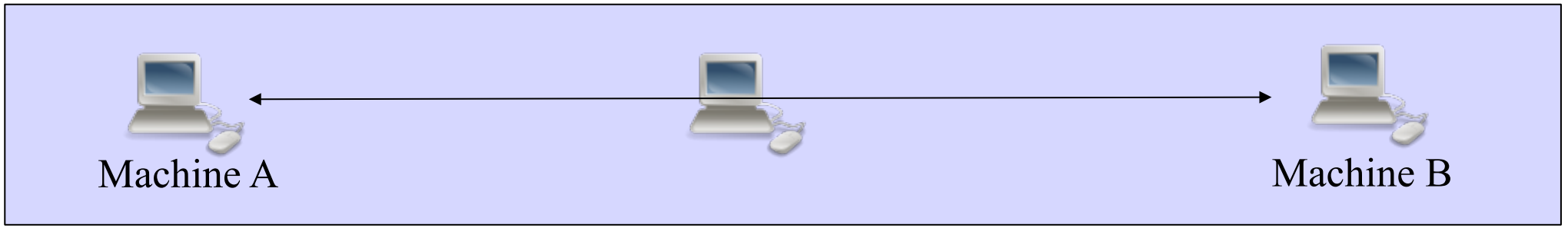


Attaques réseaux : Faiblesse d'authentification

- Génération de l'ISN TCP
  - Le standard (RFC 793) indique qu'il faut incrémenter l'ISN de 1 toutes les 4 microsecondes
  - En réalité, l'incrément peut (ou pouvait) facilement être deviné
    - Maintenant : ISN --> génération aléatoire
  - Procédé du pirate :
    - Ouvrir des connexions réelles (par ex SMTP/POP) → obtenir des ISN et des échantillons d'incréments
    - Lancer la connexion forgée en utilisant le dernier ISN plus un incrément déduit des échantillons
    - Lancer une multitude de connexions forgées avec des incréments variables

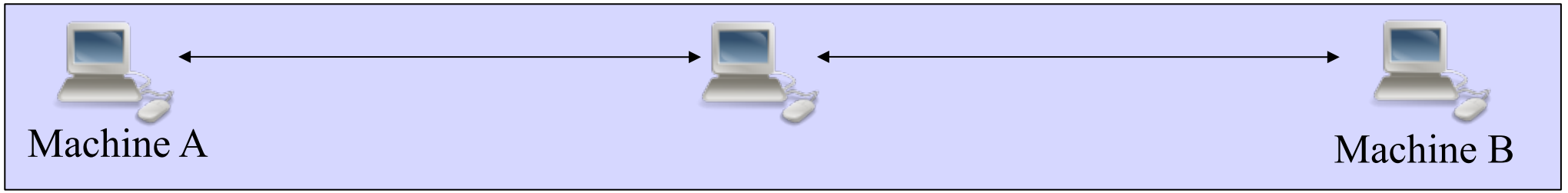
Attaques réseaux : Faiblesse d'authentification

- Attaque Man-In-The-Middle
  - Insérer la machine pirate entre les machines A et B
  - Différents types
    - Relais transparent
      - La machine pirate transforme les données à la volée
      - Rester transparent, comporte comme un routeur, A et B reste en relation
      - Sniffing + modification des données



Attaques réseaux : Faiblesse d'authentification

- Relais applicatif
  - La machine pirate l'échange entre les machine A et B
  - A discute avec le pirate et le pirate discute avec B



Attaques réseaux : Faiblesse d'authentification

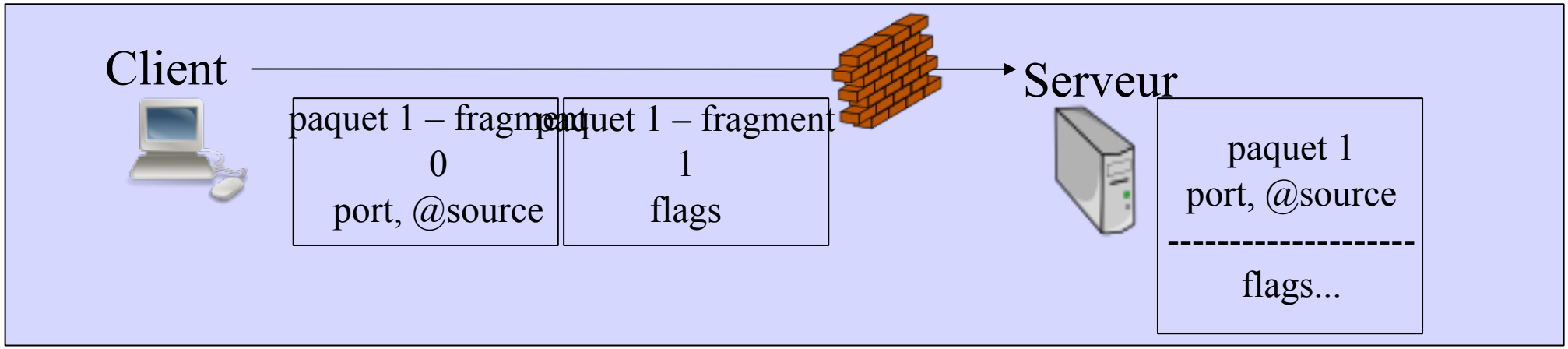
- Hijacking
  - La machine pirate utilise la session engagée entre A et B
  - Permet de rediriger un flux TCP en outrepassant les authentifications
  - Phase 1 : sniffing, déterminer qu'une authentification à eu lieu
  - Phase 2 : IP spoofing avec désynchronisation des ISN
  - Phase 3 : ARP spoofing

Attaques réseaux : Faiblesse d'implémentation

- Faiblesse d'implémentation ou bogues
  - Attaques sur les systèmes d'exploitation
  - Utilisation
    - failles dans les protocoles
    - failles dans les programmes : exploit

Attaques réseaux : Faiblesse d'implémentation

- Failles dans les protocoles
  - Même principe que les attaques pour passer les pare-feu



Attaques réseaux : Faiblesse d'implémentation

- Faille dans les programmes : exploit
  - Les logiciels contiennent des défauts
  - Les défauts peuvent être exploités par des pirates
  - Un « exploit » est la méthode, le script, qui permet d'exploiter le défaut
  - Les exploits sur les serveurs sont les plus dangereux :
    - Peuvent être fait à distance
    - Les serveurs ont souvent des privilèges élevés

Attaques réseaux : Faiblesse d'implémentation

- Failles conceptuelles
  - Exemple classique : directory traversal
    - Les documents d'un serveur web sont accessibles depuis une racine.
    - Si le serveur ne vérifie pas les URL, on peut accéder à d'autres fichiers

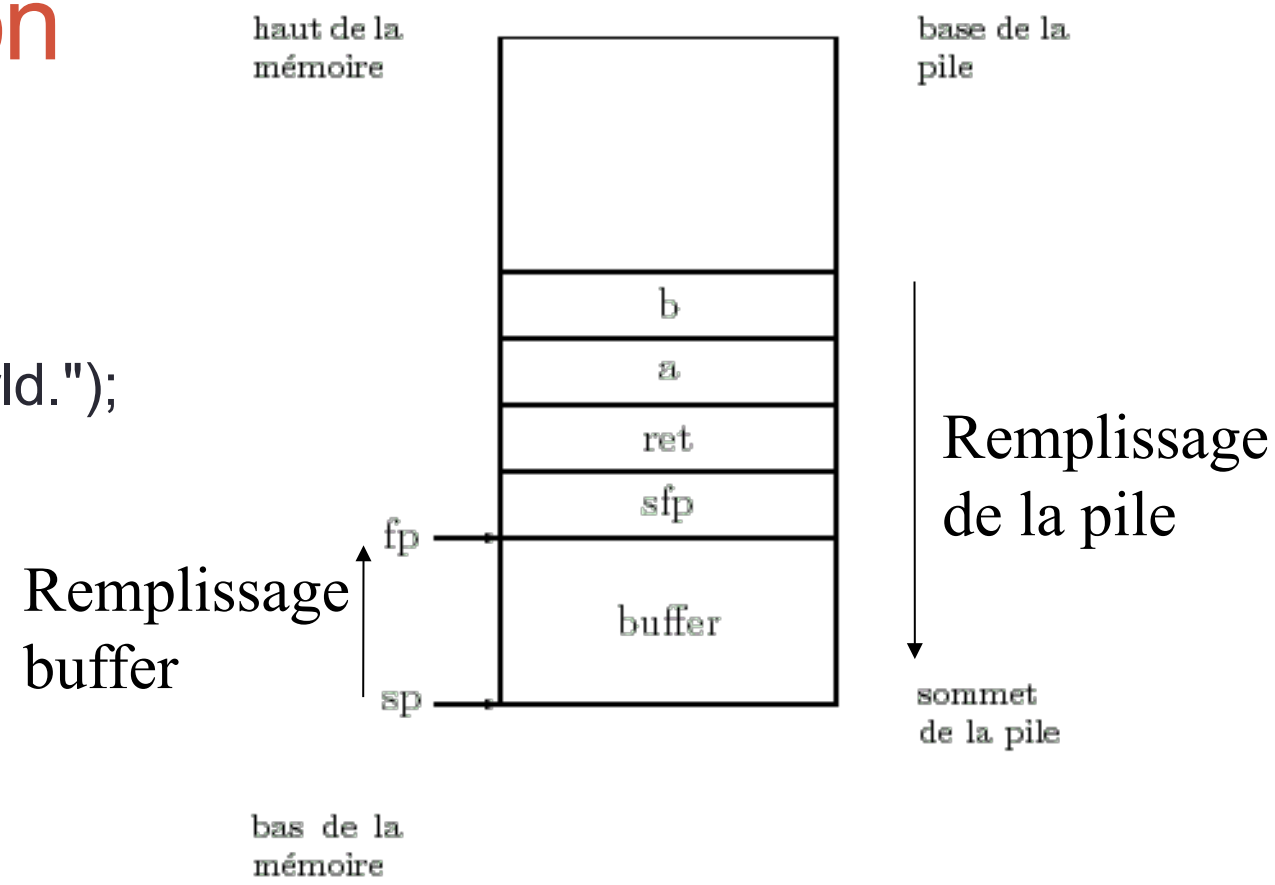
- Failles techniques
  - Classique : le buffer overflow
    - Si un programme ne vérifie pas la quantité de données qu'il reçoit, il risque d'écraser une zone mémoire qui contient des variables, du code ou des adresses de saut
    - En connaissant bien l'architecture de la machine on peut fournir du code machine qui sera exécuté

Attaques réseaux : Faiblesse d'implémentation

- Rappel: la pile
  - La pile sert à stocker des informations momentanément
  - On retire les informations dans l'ordre inverse des dépôts
    - C'est une pile !
  - Opérations effectuées sur la pile lors d'un appel de procédure:
    - 1. Les paramètres de la procédure sont déposés sur la pile.
    - 2. L'adresse de retour est déposée sur la pile.
    - 3. La valeur actuelle du pointeur de trame est déposée sur la pile.
    - 4. Une zone de mémoire pouvant contenir toutes les variables locales de la procédure est réservée sur la pile.
    - 5. Le début de cette zone est stockée dans le pointeur de trame.

Attaques réseaux : Faiblesse d'implémentation

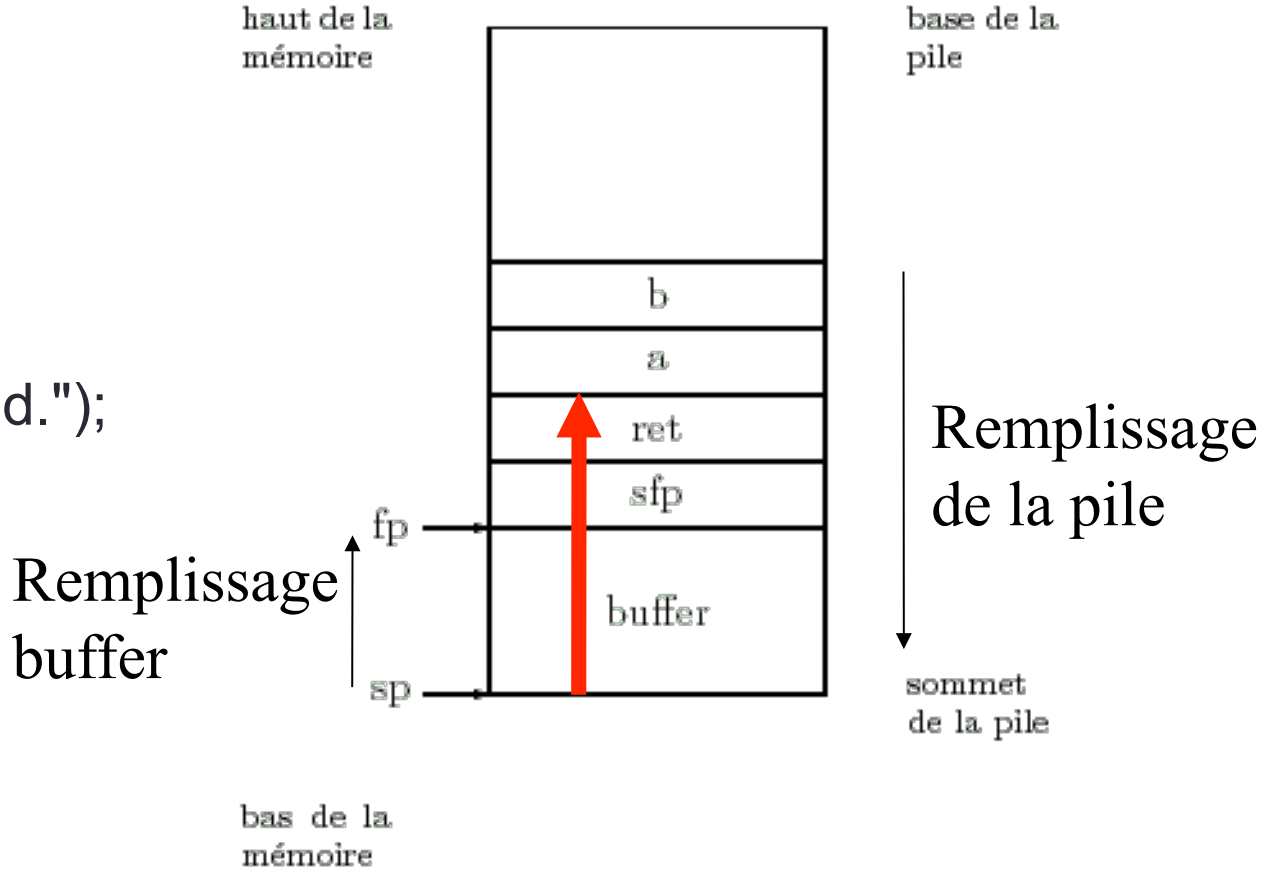
- Exemple
- void f(int a, int b) {
  - char buffer[10];
  - strcpy(buffer,"hello world.");
- }
- void main() {
  - f(1,2);
- }



- sp: pointeur de pile,
- fp: pointeur de trame,
- sfp: pointeur de trame précédant sauvegardé

Attaques réseaux

- Exemple (suite)
- void f(int a, int b) {
  - char buffer[10];
  - strcpy(buffer,"hello world.");
- }
- void main() {
  - f(1,2);
- }



- Il est difficile de deviner l'avancement de la pile et de choisir « ret »

Attaques réseaux

- Exemple
  - Le serveur web MS-IIS avait un buffer overflow sur les URL(1999/2001)
  - NetMeeting avait un buffer overflow sur l'adresse à appeler
  - libjpeg
  - ...

Attaques réseaux : Faiblesse d'implémentation

- Autre Exemples
  - L'attaque +++ATHZero
    - Vise certains modems compatibles Hayes.
    - Lorsque ce type de modem reçoit la commande +++ATH0, il risque de se déconnecter.
  - L'attaque Cisco ® 7161
    - Se connecter au port 7161 d'un routeur Cisco ® et d'envoyer un retour chariot.
    - Le routeur peut alors planter
    - A vérifier...

Attaques réseaux : Faiblesse de configuration

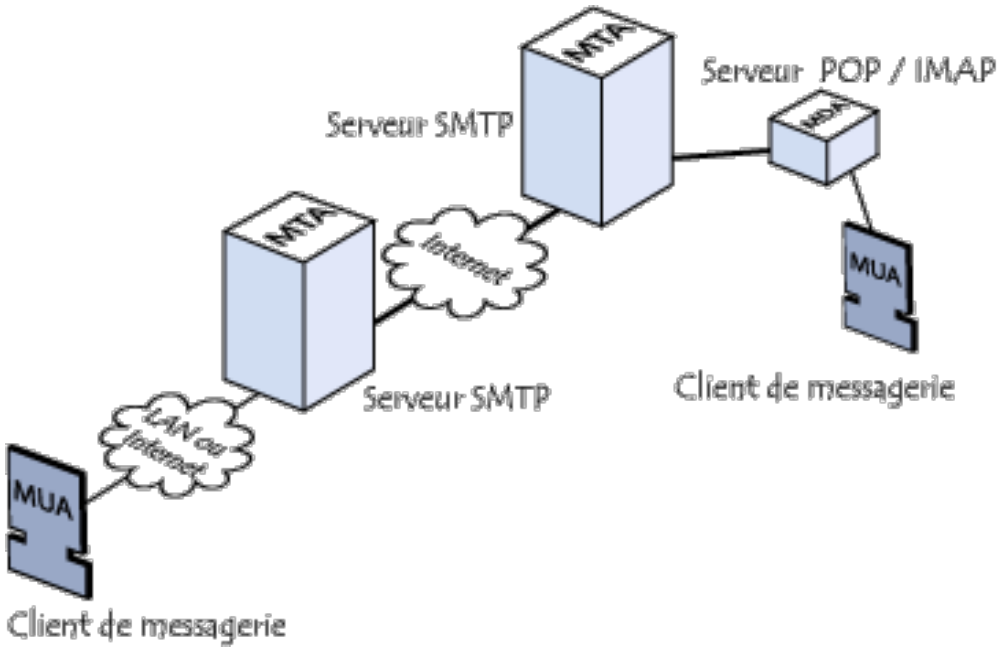
- Exploitation d'erreurs de configuration du système
  - OS des machines
  - OS des éléments du réseau (routeurs, switchs, hub...)
- Politique de mots de passe trop laxiste
  - Mots de passe appartenant à un dictionnaire
  - Dictionnaire spécialisé

Plan

- I-Attaques sur l'information
- II-Attaques réseaux
  - faiblesses des protocoles réseaux
    - cartographie du réseaux, identification des systèmes, écoute du trafic
    - sauter le firewall, commutateur, DoS
  - faiblesses d'authentification(ARP, IP, mot de passe)
  - faiblesse d'implémentation, bogues (TCP syn, bogues IP/TCP, OS)
  - faiblesse de configuration (OS, mots de passe)
- III-Attaques indirectes
  - Mails
  - Virus, vers, cheval et autres animaux

Attaques indirectes : mail

- Envoi d'un email : protocole SMTP
  - le message est envoyé au serveur de courrier électronique chargé du transport (nommé MTA pour Mail Transport Agent), jusqu'au MTA du destinataire
  - les MTA communiquent entre-eux grâce au protocole SMTP
  - Le serveur MTA du destinataire délivre alors le courrier au serveur de courrier électronique entrant (nommé MDA pour Mail Delivery Agent)
  - Le MDA stocke le courrier en attendant que l'utilisateur vienne le relever (protocole POP ou IMAP)



http://www.commentcamarche.net/courrier-electronique/fonctionnement-mta-mua.php3

Attaques indirectes : Attaque par mail

- Email forgé
  - Le protocole SMTP (Simple Mail Transfer Protocol) RFC 821, 1982
  - SMTP n'utilise aucune authentification
  - il est facile de forger des messages : utilisez telnet
  - SMTP utilise des connexions TCP sur le port 25
  - Quelques simples commandes comme :
    - HELO (annonce d'un serveur)
    - Mail From: (définition expéditeur)
    - Rcpt To: (définition destinataire)
    - Data: (définition du contenu)

Attaques indirectes : Attaque par mail

```
telnet iupmime.lium.univ-lemans.fr 25
Trying 128.178.7.12...
Connected to iupmime.lium.univ-lemans.fr
Escape character is '\^]'.
220 iupmime.lium.univ-lemans.fr ESMTP
helo prt-sylvain.lium.univ-lemans.fr
250 iupmime.lium.univ-lemans.fr
mail from:mephisto@hell.com
250 ok
rcpt to:sylvain.meignier@univ-lemans.fr
250 ok
data
have a nice day
.
250 ok 994426415 qp 14851
quit
221 iupmime.lium.univ-lemans.fr
Connection closed by foreign host.
```

Attaques indirectes : Attaque par mail

- Principe
  - Le message est déposé dans un serveur SMTP
  - Le serveur va le déposer dans le serveur plus proche de la destination
    - Interrogation du DNS → donne l'adresse du serveur SMTP responsable pour le domaine destination
  - Le serveur SMTP du domaine cible va déposé le massage dans la boite du destinataire
- Chaque serveur ajoute un en-tête au message
- Le serveur qui reçoit le message initialement note :
  - Le commentaire de la commande hello
  - L'adresse IP de l'émetteur du message
  - L'heure de réception
- Il est souvent possible de retrouver l'auteur du message

Attaques indirectes : Attaque par mail

- SPAM
  - E-mail non-sollicité, non-ciblé, à très grand tirage
  - L'adresse source est toujours falsifiée (représailles)
  - Message déposé dans + de 100 serveurs SMTP avec une liste de + 10k destinations
  - Message envoyé à chaque destinataire
  - Problèmes :
    - Les serveurs abusés sont surchargés (souvent plus de 24h)
    - Les disques se remplissent de logs et de messages (risque de blocage)
    - Le mail de l'admin est inondée de messages d'erreurs (adresses invalides)
    - L'ISP peut menacer de couper la ligne
    - Inclusion dans listes noires

Attaques indirectes : Attaque par mail

- Pourquoi le SPAM est il possible ?
  - Relais ouverts
    - Permet à des tiers appartenant à des réseau quelconques d'envoyer des courriers électronique
    - Utilisés par les spammeurs, permet de masquer l'origine des messages
  - Pour qu'un serveur SMTP ne fasse pas de relais pour des tiers (open relay) il faut configurer deux règles:
    - L'expéditeur ou le destinataire doit être local
    - Seules les machines locales ont le droit de spécifier des expéditeurs locaux.
  - Les spammers essaient de passer entre les gouttes en utilisant des formes spéciales d'adresses (!<>&)

Attaques indirectes : Attaque par mail

- Le Mail Bombing
  - Envoyer un nombre faramineux d'emails (plusieurs milliers) à un ou des destinataires.
  - L'objectif étant de :
    - Saturer le serveur de mails
    - Saturer la bande passante du serveur et du ou des destinataires,
    - Rendre impossible aux destinataires de continuer à utiliser l'adresse électronique.
  - Logiciels permettant de réaliser le mail bombing.

Attaques indirectes : Attaque par mail

- Virus, Ver, Trojan et autres animals
  - Type
    - Virus: programme qui se propage à l'aide d'autres programmes
    - Ver: programme autonome
    - Cheval de Troie: Programme utile qui contient un programme malveillant (ou ce dernier par abus de langage)
      - exemples : sendmail, openssh, tcpdump
    - Backdoor: accès caché à un ordinateur
  - Effet des Virus
    - Perte de données
    - Perte de temps de travail
    - Perte d'image de marque
    - Perte de fonctionnalité (e-mail ou systèmes bloqués)
    - Nouvelles fonctionnalités (serveur de spam!)
    - Perte de confidentialité (c.f. SirCam, BadTrans, Bugbear)

Attaques indirectes : Virus

- Evolution des Virus
  - Epoque Classique:
    - Propagation passive par échange de disquettes
    - Propagation lente d'ou besoin d'efficacité
    - 1er virus connu: 1981 sur Apple II ?
    - 1986, le premier virus informatique voit le jour au Pakistan ?
    - Furtivité
      - Simple:
        - le virus compresse le fichier original, crée un fichier infecté de même taille
      - Sophistiqué:
        - Le virus modifie le système de manière à ne plus être visible
        - Il modifie les routines de lecture de fichiers pour qu'elles ne révèlent pas le virus
        - Exemples:
        - Brain: infecte le boot sector mais garde une copie originale. Il redirige les accès au boot sector vers la copie
        - Frodo: modifie les routines d'accès aux fichiers, chckdsk détruit les fichiers!

Attaques indirectes : Virus

- Polymorphisme
  - Le virus se modifie à chaque infection de manière à être méconnaissable
  - Une partie du virus peut être chiffrée avec une clé différente à chaque fois
  - Le reste doit être modifié tout en gardant la même fonctionnalité (insertion d'opérations nulles, remplacements équivalents, différents algorithmes)
  - Exemple: Tequilla (1991, Suisse)
- Epoque Moderne
  - Les virus modernes utilisent Internet pour se propager activement
  - Il peuvent infecter la planète en quelques heures
  - Souvent simples et faciles à détecter
  - Efficaces, car ils se propagent plus vite que les anti-virus peuvent être mis à jour
  - Active-Mail
    - Message qui s'exécute tout seul lors de la visualisation, sans besoin de cliquer. Possible grâce à des défauts dans les logiciels de messagerie

Attaques indirectes : Virus

- Exemples
  - Melissa
  - Loveletter, aka « I love you »
    - Message avec attachement en script VBS
    - Double extension de fichier pour faire croire que c'est du texte: iloveyou.txt.vbs
    - Envoie une copie de lui-même à tous les membres du carnet d'adresses
    - Se propage aussi par IRC en modifiant les fichiers le d'initialisation (mIRC)
    - Modifie la page de démarrage IE
    - Remplace les fichiers son et image par lui-même

Attaques indirectes : Virus

- Sircam
  - Sircam est un virus qui se propage par email et par les disques partagés
  - Pour se propager par e-mail il infecte un fichier local et l'envoie comme attachement à toutes les adresses e-mail qu'il trouve sur la machine.
  - perte de confidentialité
- BugBear (septembre 2002)
  - Se propage comme active-mail en utilisant des failles de MS-IE pour exécuter automatiquement un attachement
  - Infecte les fichiers accessibles sur des partages réseau
  - Installe un backdoor (port 36794)
  - Arrête tous les antivirus actifs sur la cible
  - Envoie une copie des mots de passe enregistrés localement à une vingtaine de bals
  - Installe un espion de clavier

Attaques indirectes : Virus

- SQL Slammer, janvier 2003
  - Il s'agit d'un ver qui profite d'un buffer overflow pour infecter des serveurs SQL et leur faire infecter d'autres serveurs
  - Le ver arrive dans un paquet UDP de 376 octets sur le port 1434
  - Il contient un petit programme qui génère des adresses IP aléatoires (à l'aide de l'horloge du système)
  - Une copie du paquet est envoyée à chaque adresse générée
  - Comme c'est de l'UDP le ver peut envoyer les paquets à plein débit, sans avoir à négocier une connexion TCP
  - C'est une des raisons qui rend ce ver si virulent

Attaques indirectes : Virus

- Virus spéciaux:
  - Le Canular (Hoax)
    - Décrit une menace catastrophique
    - Contient aucune référence à des sources d'infos fiables (mais des réf. floues)
    - Demande à être envoyé à toutes les personnes que vous connaissez
  - Joke : Programme amusant que vous allez envoyer à tous vos amis
  - Publicité virale (idem)
  - Dégâts
    - Canular: perte de temps (ou plus, cf mtx hotline)
    - Joke: Vecteur idéal pour virus. Donne de mauvaises habitudes aux utilisateurs
    - Pub: Consommation de bande passante

Attaques indirectes : Virus

- Backdoors
  - Programmes qui permettent de gérer des ordinateurs à distance, à l'insu de son utilisateur
  - Installés par des chevaux de Troie et souvent classifiés comme tels
  - Caractéristiques
    - Taille: plus il est petit, plus il est facile à installer
    - Fonctionnalités: téléchargement d'autres programmes, espionnage réseau, écran, clavier.
    - Mode de communication: Attente sur un port TCP ou UDP prédéfini.
    - Mieux: port aléatoire communiqué par e-mail ou IRC.
    - Encore mieux: communication par ICMP, chiffrement.
  - Exemple : BackOrifice, NetBus, SubSeven