— Sécurité des réseaux —

Université de Thiès

UFR Sciences et Technologies

Enseignant : Cheikh SARR

Professeur Titulaire
Réseaux et télécommunications

Contact : csarr@univ-thies.sn

1-Introduction à la sécurité des réseaux

Introduction

- Sécurité des réseaux
  - Maillon important de l'administration des réseaux
- Difficulté est de trouver un **compromis** entre
  - Besoin d'ouverture des réseaux pour accéder à de nouvelles ressources
  - Protéger les informations
- Application d'une stratégie de sécurité réseau
  - Définit les directives concernant les activités et les ressources nécessaires à la sécurisation d'un réseau d'entreprise.
- **Nous nous intéressons à la sécurité informatique au niveau des réseaux**

Importance de la sécurité

- Les réseaux ont grandi en taille et en importance des données stockées
- Internet
  - Recherche de l'équilibre entre ouverture et protection du système et des données
- Augmentation des menaces
  - Outils plus sophistiqués et donc plus complexes
- Dans ce cours nous verrons
  - Développement de stratégie de sécurité au niveau des organisations
  - Sécurité au niveau des LAN
  - Sécurité au niveau des réseaux IP et WAN

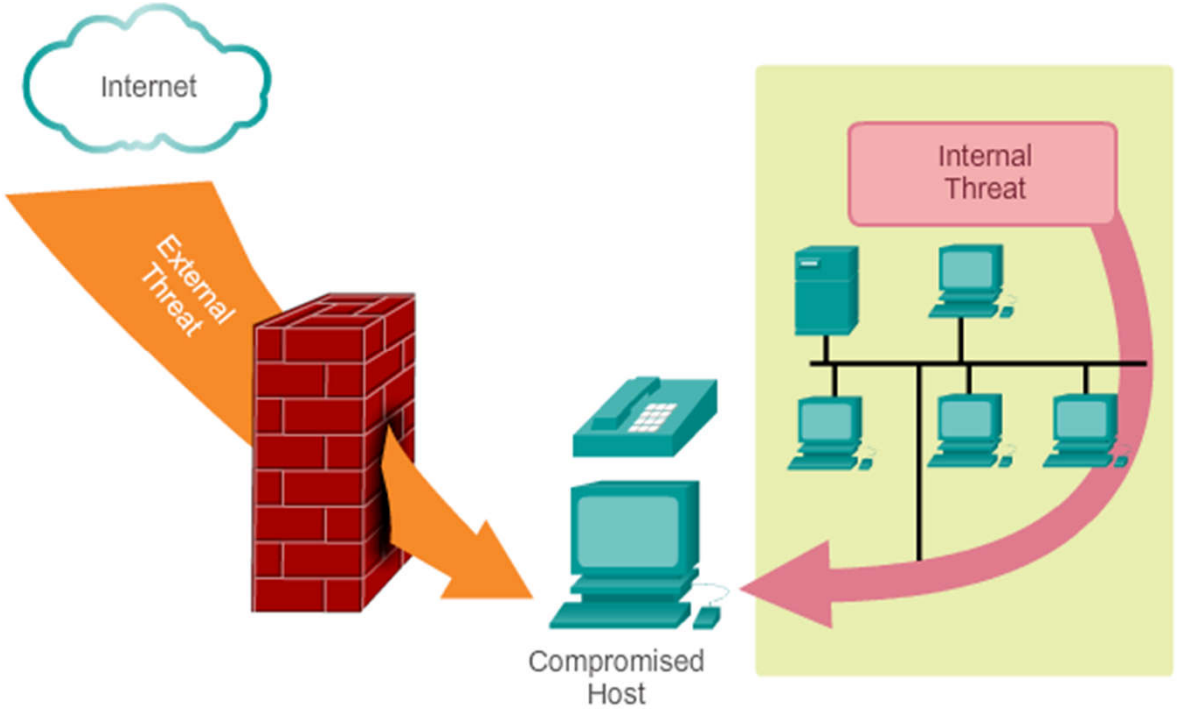
Définition et organisation

- La sécurité informatique est l'ensemble des techniques mises en œuvre afin d'assurer la protection :
  - Des informations (données)
  - Du matériel
  - Des logiciels
- Elle se divise en quatre grandes catégories
  - L'analyse des risques
  - La définition d'une politique de sécurité
  - La mise en place de techniques de sécurité
  - La mise en place de tests de vérification

Critères de sécurité

- **Disponibilité**
  - Garantie de l'accessibilité des informations en temps voulu
- **Intégrité**
  - Garantie que les éléments sont exacts et complets
- **Confidentialité**
  - Garantie que les seuls personnes autorisées ont accès à l'information
- **Traçabilité ou Preuve**
  - Garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables

Provenance de menaces



- Les menaces des systèmes peuvent provenir
  - D'un utilisateur ou d'un programme **interne**
  - D'un utilisateur ou d'un programme **externe** (contournement du système de protection)

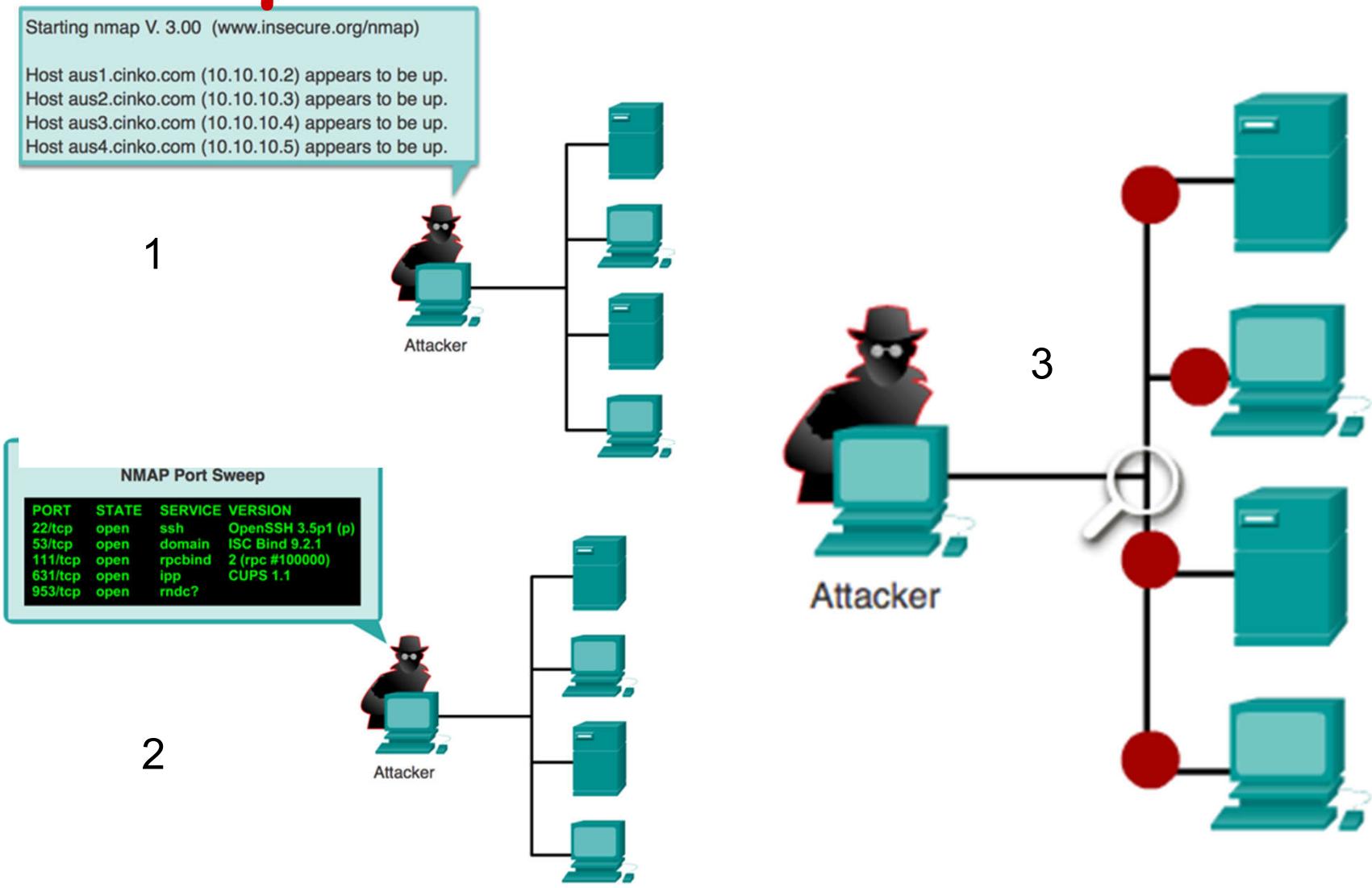
Types d'attaques réseaux

- Il sont au nombre de quatre
  - **Reconnaissance** : découverte non autorisée des systèmes, de leurs adresses et de leurs services
  - **Accès** : accéder à un périphérique pour lequel l'intrus ne dispose pas d'un compte ou d'un mot de passe autorisé
  - **Déni de service** : désactivation ou altération d'un réseau, des systèmes ou des services dans le but de refuser le service prévu aux utilisateurs normaux
  - **Vers, virus et chevaux de troie** : logiciels malveillants pouvant être installés sur un ordinateur hôte dans le but d'endommager ou d'altérer un système

Attaques de reconnaissance

- Requêtes Internet
  - Découvertes des adresses IP en utilisant les outils tels que *nslookup* et *whois*
- Balayage ping
  - Utilisation des requêtes *ping* pour savoir si ces équipements sont accessibles
- Balayage de ports
  - Outils de balayage de ports pour connaître les services réseaux actifs (HTTP, SMTP, DHCP)
- Analyseurs de paquets
  - Interception et analyse des paquets pour y rechercher des informations confidentielles telles que des mots de passe ou des comptes utilisateurs

Attaques de reconnaissance



Attaques d'accès

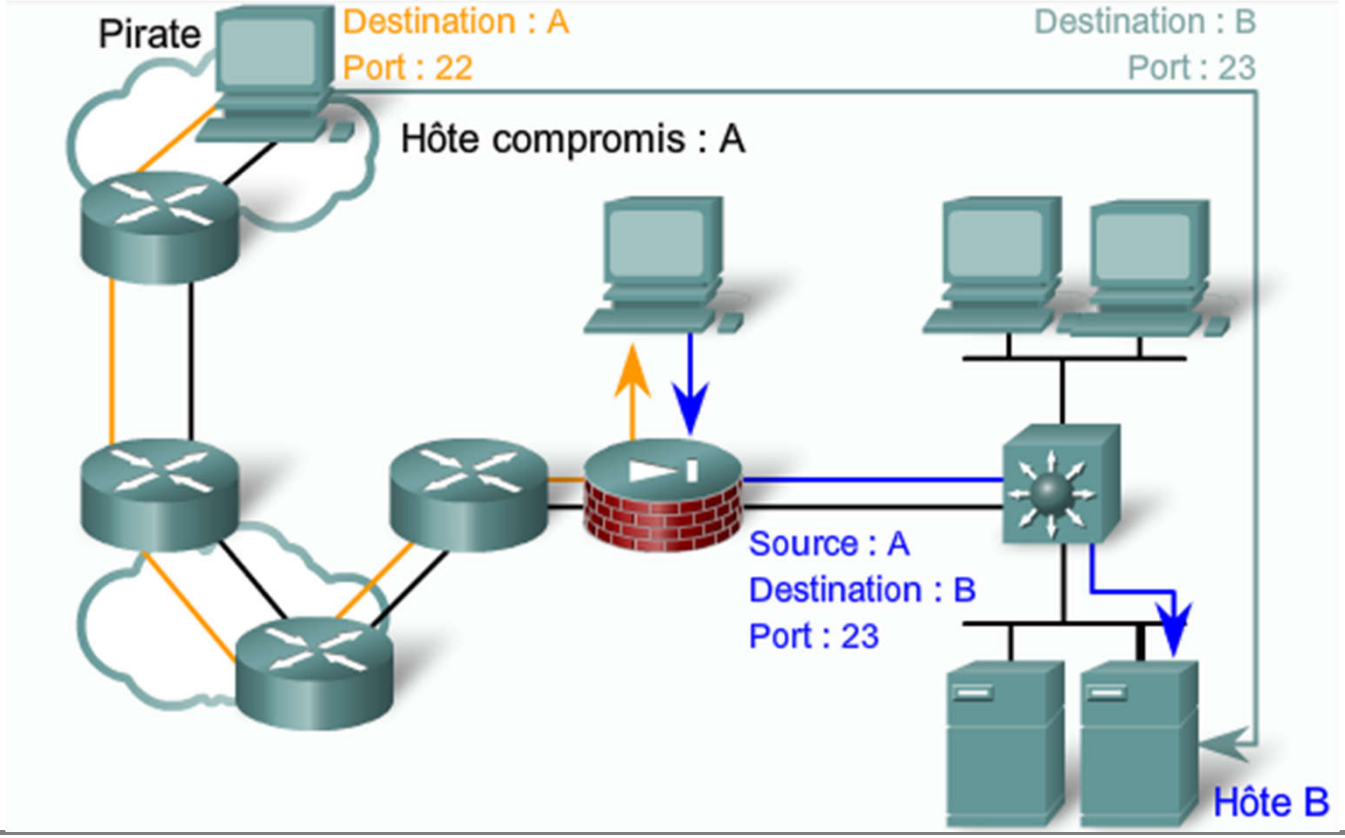
- Attaques de mot de passe
  - Analyseur de paquets pour récupérer les mots de passe qui circulent en clair
  - Force brute : utilisation des combinaisons possibles
- Redirection de ports
  - Utiliser un équipement externe accessible et lui installer un logiciel de redirection de ports pour accéder à une machine d'un réseau local
- Homme du milieu
  - Interposition d'un tiers entre deux hôtes légitimes afin de récupérer des informations sensibles

Attaque par force brute

- Elle s'établit sur des systèmes présentant des codes ou des mots de passe
  - Utiliser toutes les combinaisons possibles jusqu'à trouver le bon code
- Solution : imposer des codes assez long composés de lettres et de chiffres
  - Exemple : Mot de passe de 5 lettres, il existe 26^5 possibilités soit : 11 881 376 possibilités
  - Combien de possibilités aura-t-on si on utilise aussi bien des lettres que des chiffres ? des lettres majuscules, minuscules et des chiffres ?

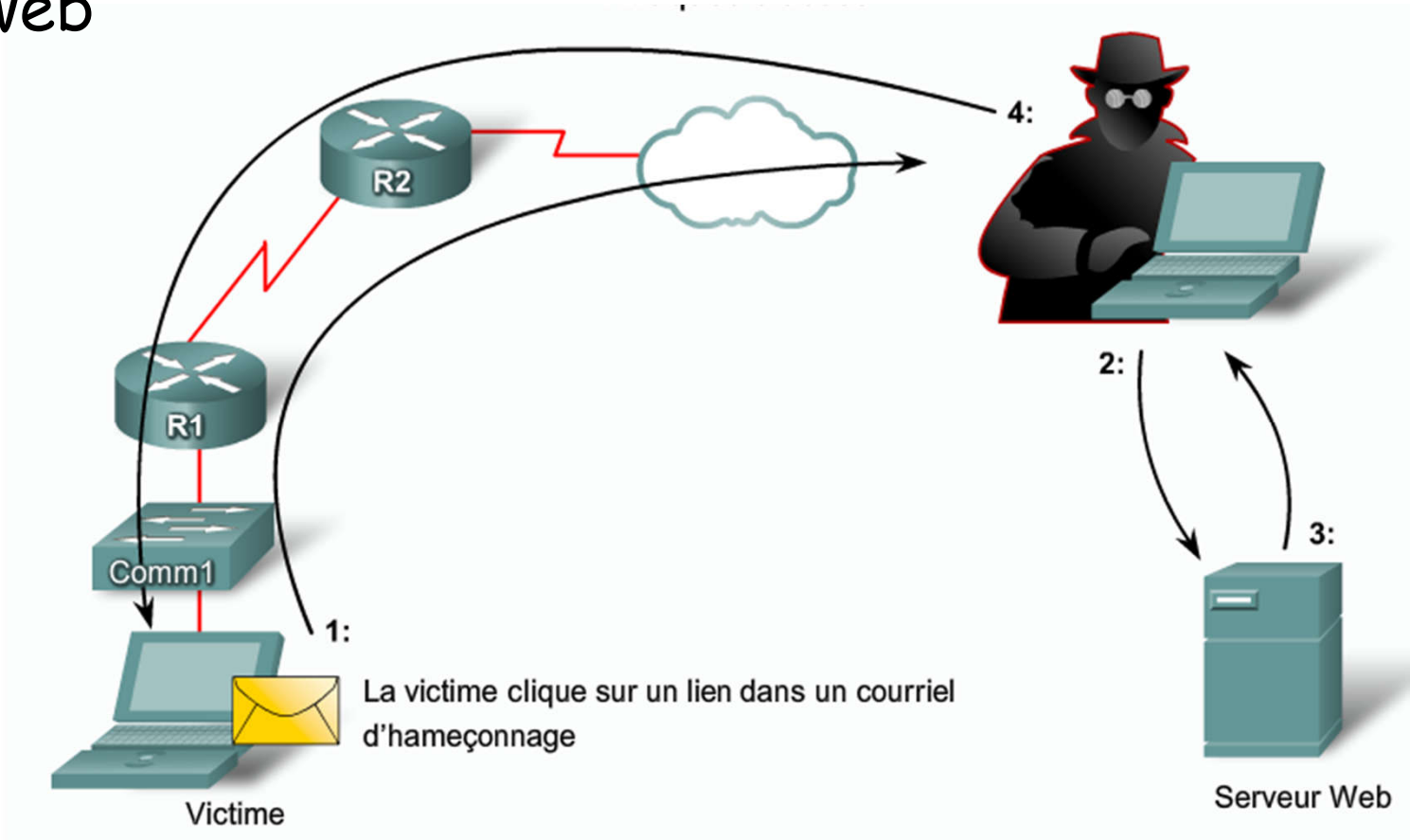
Redirection de ports

- Redirection à partir du **serveur A** qui se trouve sur la DMZ et normalement accessible



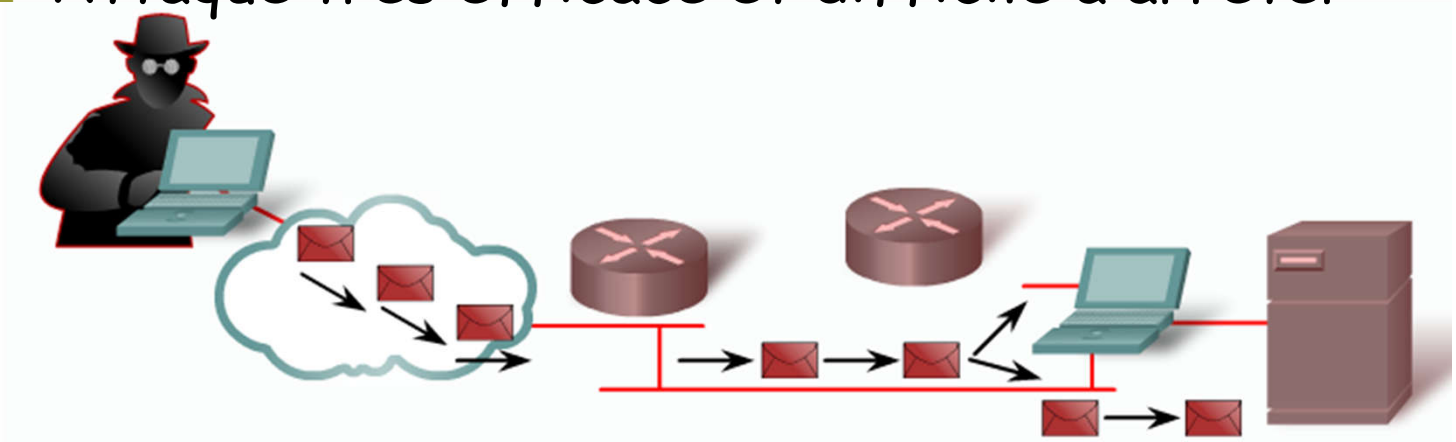
Homme du milieu

- Intercepte les transactions destinées au serveur web



Attaques par déni de service

- Vise à rendre une application informatique incapable de répondre aux requêtes de ses utilisateurs
  - Tentatives de connections simultanées en nombre très important ce qui provoque l'arrêt de la machine serveur
  - Attaque très efficace et difficile à arrêter

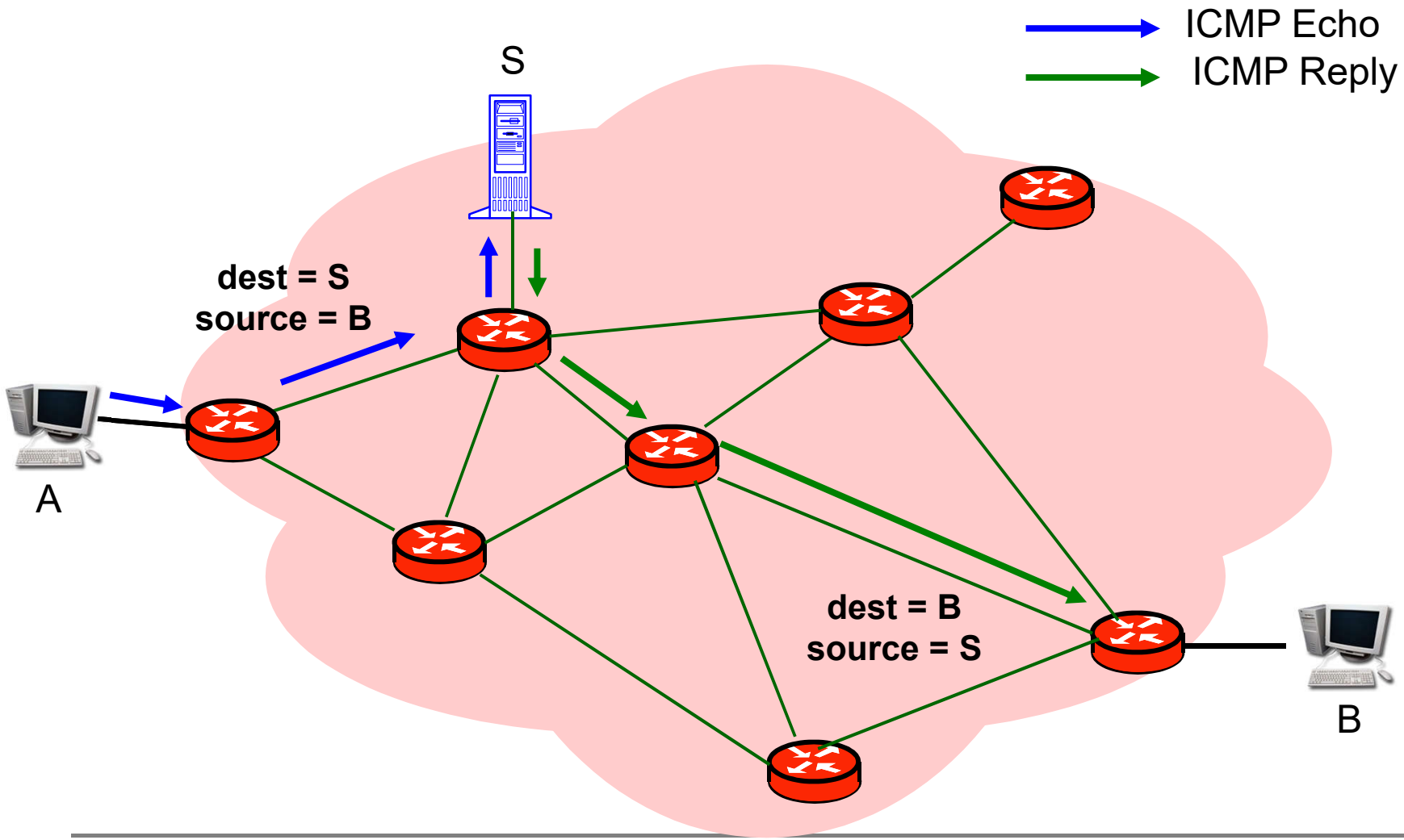


Les attaques par déni de service empêchent l'utilisation d'un service par les personnes autorisées en épuisant les ressources du système.

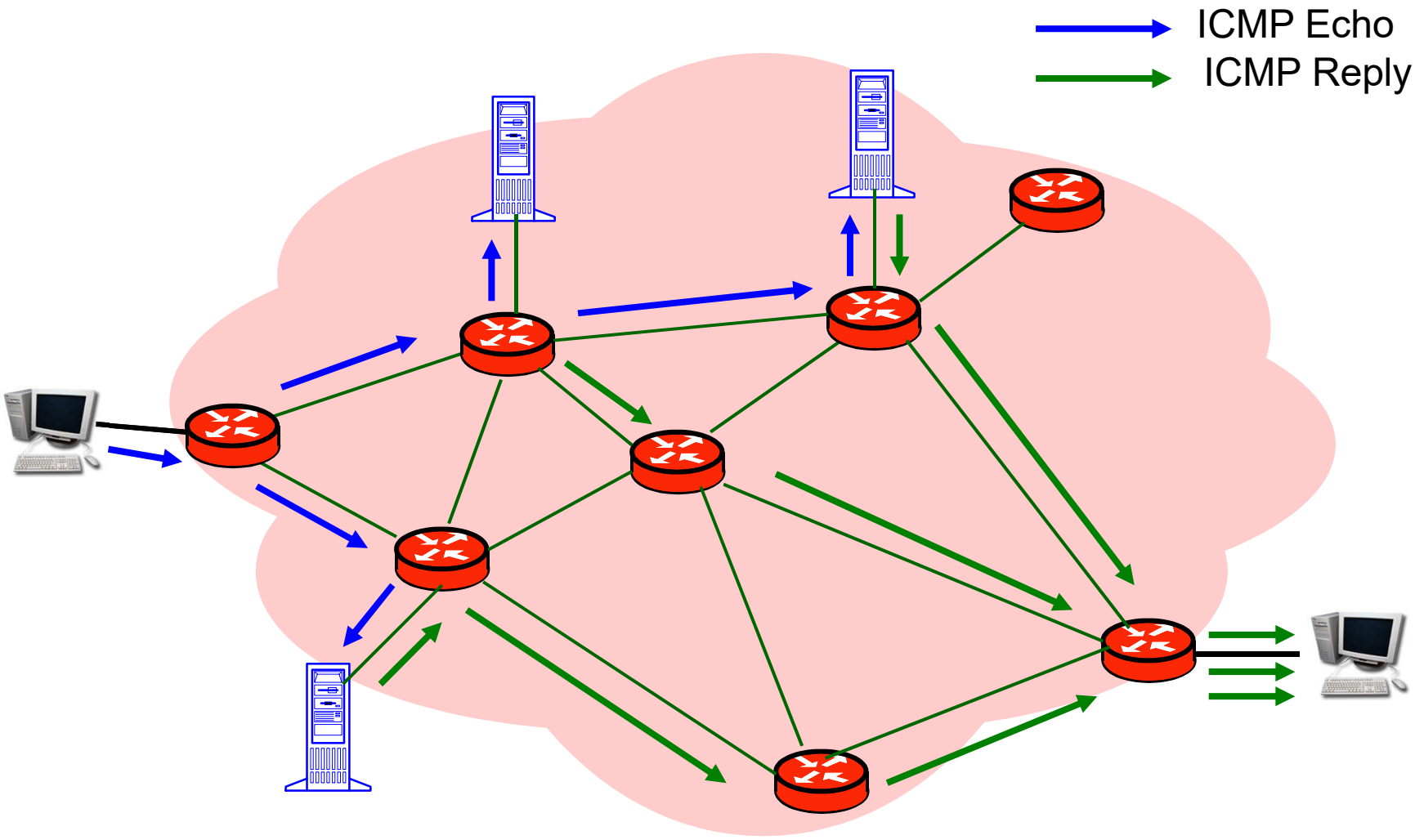
IP spoofing

- Lorsqu'une requête PING (ICMP REQUEST) est envoyé vers un serveur il répond à la machine source par une réponse PING (ICMP ECHO)
- Avec l' IP spoofing, **on vole l'adresse** d'une machine B quelconque du réseau
- Envoie plusieurs milliers de requêtes PING depuis une machine A vers un serveur S avec comme adresse source celle de B
- Les réponses sont envoyés à la machine B qui finit par « crasher » et devenir inaccessible

IP spoofing



IP spoofing distribué



Virus

- Définition
  - Programme informatique capable **d'infecter** un autre programme d'ordinateur en le **modifiant** de façon à ce qu'il puisse à son tour se **reproduire.** La notion de **reproduction** est fondamentale
- Fonctions
  - Possibilité de se reproduire par **soi-même** et de se **propager** sur un nombre important d'ordinateurs
  - Le virus va donc chercher à **détruire** ou du moins **affaiblir** le système informatique qu'il infecte
- Solution
  - **Antivirus efficace avec mise à jour régulière**

Autres types d'attaques

- **Vers**
  - Programme qui se copie d'un ordinateur à un autre. Pas d'infection comme pour les virus
- **Cheval de Troie**
  - Ouvrir une brèche sur l'ordinateur cible afin de donner un accès à un personne externe
- **Spyware**
  - Collecter et transférer des informations récupérées à l'insu de l'utilisateur
- **Spam**
  - Courriel non sollicité généralement pour de la publicité

Techniques de sécurisation

- **Durcissement de la configuration**
  - Changement des mots de passes, désactivation de services et applications inutiles
- **Logiciel antivirus**
  - Analyse des fichiers en les comparant à une base de données de virus (mise à jour de la base)
- **Pare-feu**
  - Protection des ordinateurs personnels et des réseaux d'entreprises
- **Correctifs de OS**
  - Mise à jours de patches pour réparer des failles de sécurité apparaissant sur les OS

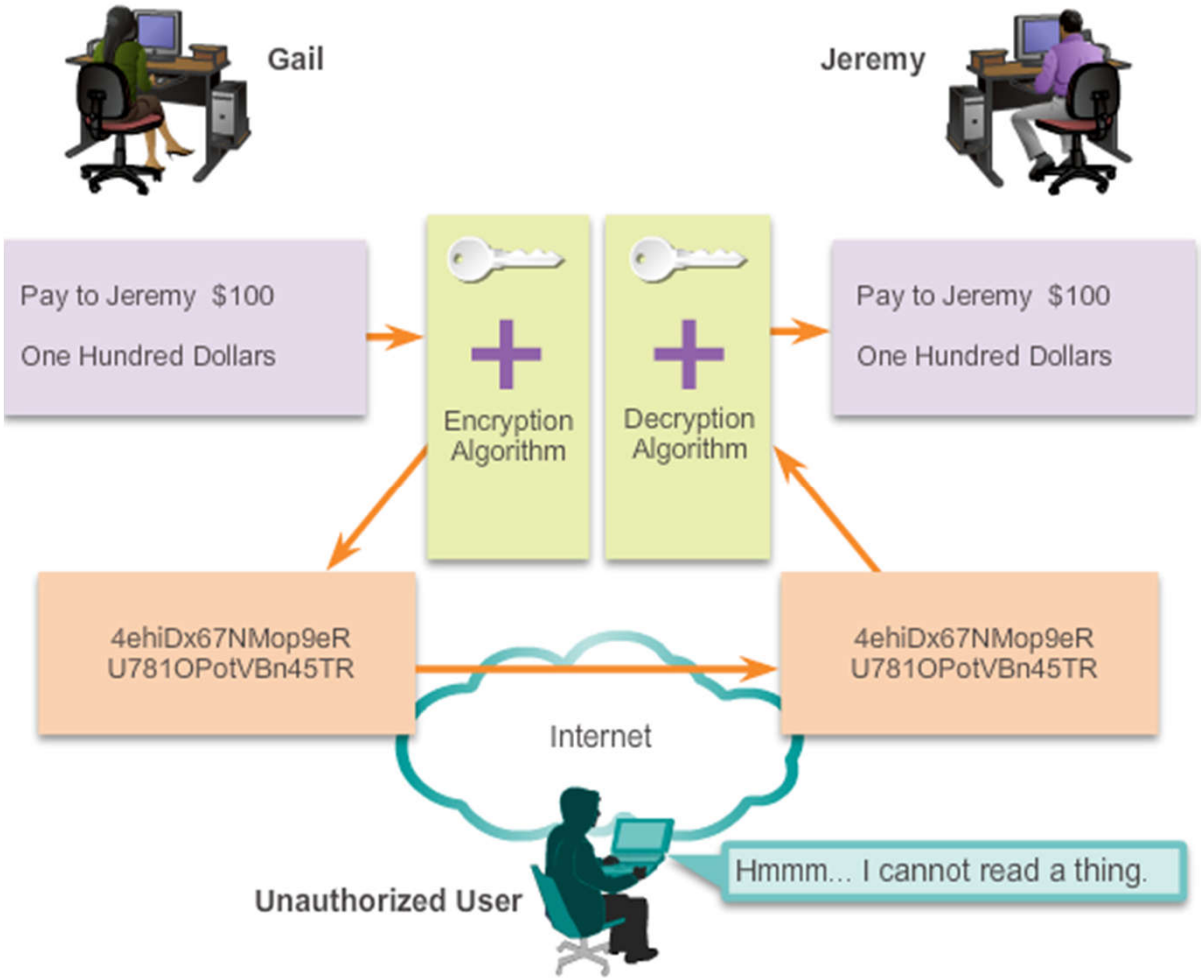
Techniques de sécurisation

- **Filtre d'URL**
  - Filtrage de certaines URL pour l'accès web
- **Serveur d'authentification**
  - Serveurs dédiés à l'authentification des utilisateurs
- **Détection d'intrusion**
  - Détecter des comportements anormaux afin de déclencher des alarmes préventives
- **Zone démilitarisée (DMZ)**
  - Zone isolée pour des serveurs spécifiques
- **Réseaux privés virtuels (VPN)**
  - Création d'un réseaux virtuel généralement sécurisé entre des ordinateurs distants

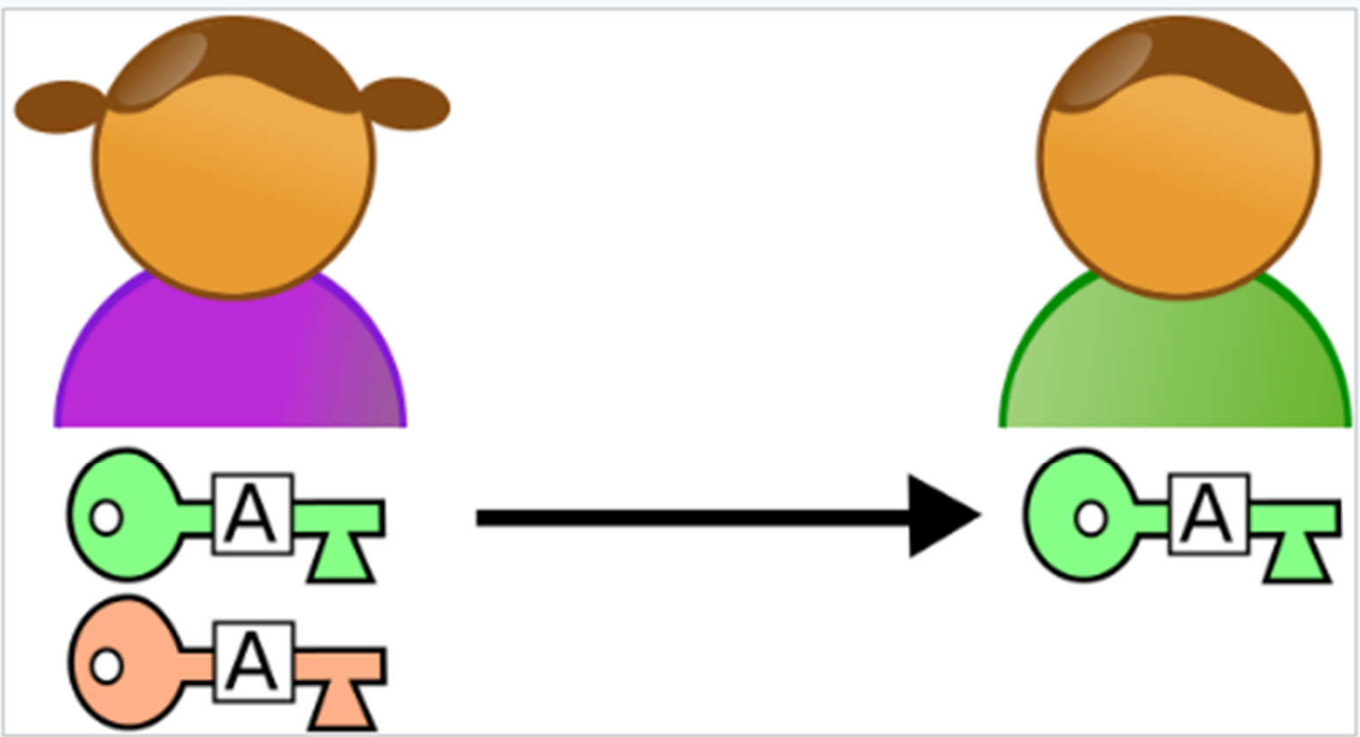
Cryptographie

- Crypter des informations pour en assurer la confidentialité entre émetteur et destinataire
  - Mécanisme de sécurité très utilisé sur Internet
  - Ex : VPN utilise un cryptage
- Cryptographie symétrique
  - Un même clé sert à crypter et décrypter les informations
  - **Ex** : AES
- Cryptographie asymétrique
  - Une clé secrète et publique sont générées. La clé publique est envoyée et sert au cryptage tandis que la clé privée sert au décryptage
  - **Ex** : RSA

Cryptographie symétrique

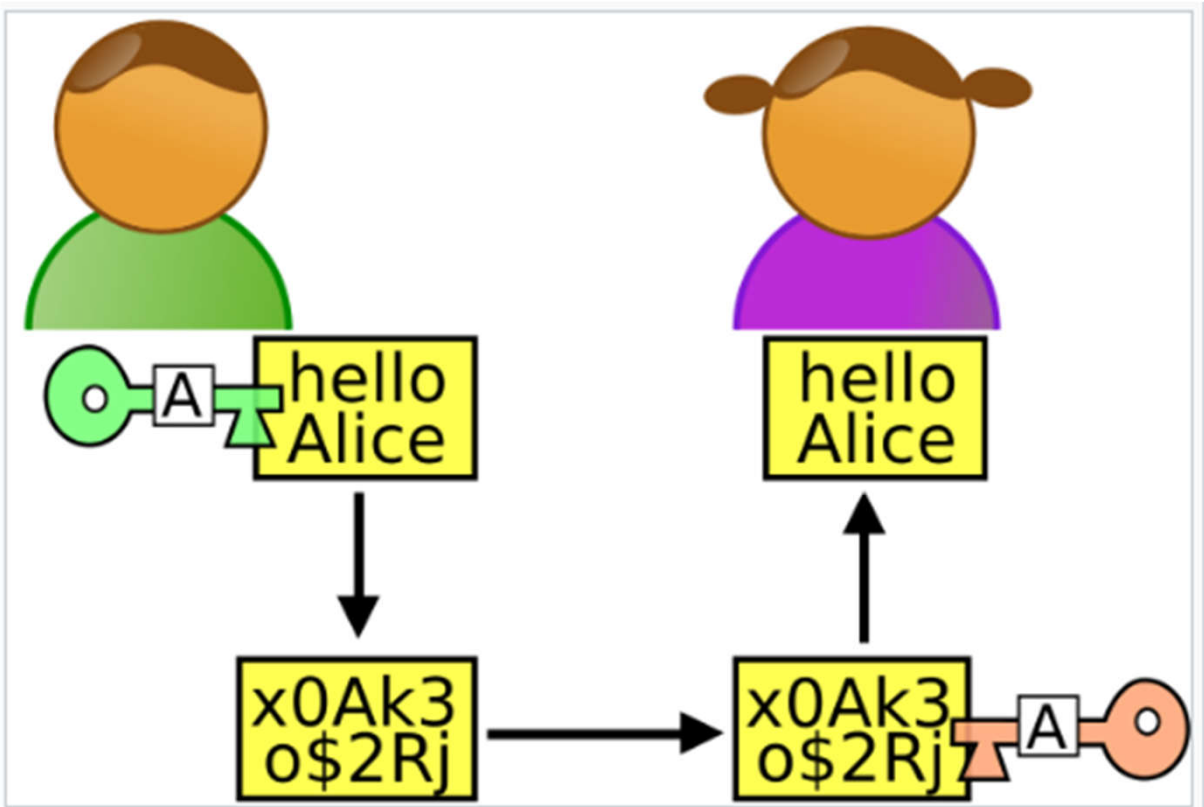


Cryptographie asymétrique (1/2)



1re étape : Alice génère deux clefs. La clef publique (verte) qu'elle envoie à Bob et la clef privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.

Cryptographie asymétrique (2/2)



2e et 3e étapes : Bob chiffre le message avec la clef publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clef privée.

Métiers liés à la sécurité

- **Technicien sécurité**
  - Gère la sécurité du réseau et des postes clients sous la supervision d'un ingénieur
- **Ingénieur sécurité**
  - Technicien sécurité plus avancé
- **RSSI**
  - **R**esponsable **S**écurité des **S**ystèmes **I**nformatiques
  - Définit la stratégie globale de sécurité d'un réseau d'entreprise et du respect des normes de sécurité
- **DSI**
  - **D**irecteur des **S**ystèmes **I**nformatiques
  - Intégrer la sécurité dans un système d'information plus global