Université de Guelma
Département Informatique

Chapitre 1 : Introduction à la Sécurité Informatique

Cours - Sécurité Informatique

3 année LMD Système d'Information

Par : Dr. M. A. Ferrag

Plan

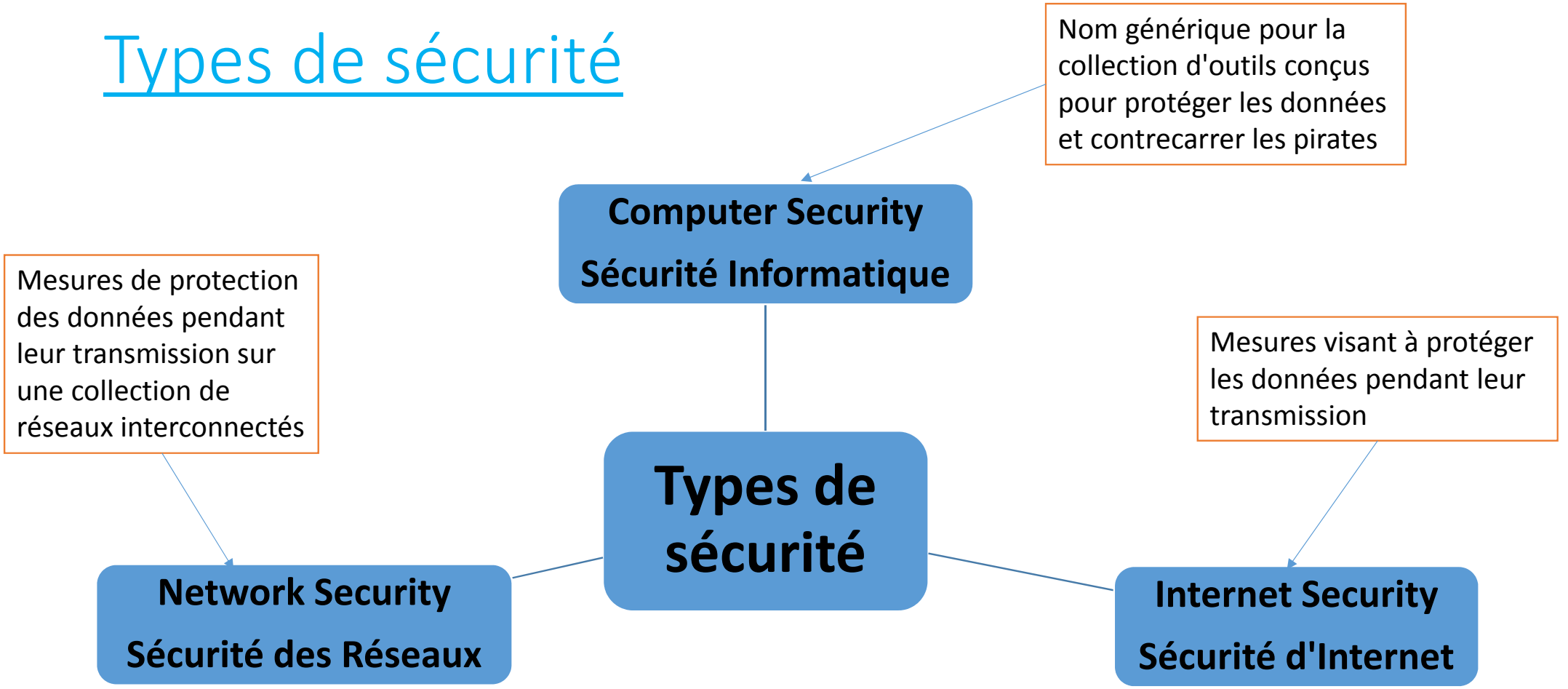
Partie 1

- Types de sécurité
- Exigences fondamentales
- Contrôle d'accès
- Types de contrôle d'accès
- Authentification
- Authentification forte (Strong Authentication)
- Autorisation
- Authentification vs. Autorisation
- Intégrité

Partie 2

- Les attaques : en temps réel
- Type des attaquants : par compétence
- Type des attaquants : par objectif
- Motivation des attaques
- Les attaques réseaux (Les plus fréquentes)
- L'attaque par rebond

Types de sécurité



Exigences fondamentales

- **Disponibilité :** *Demande que l'information sur le système soit disponible aux personnes autorisées.*
- **Confidentialité :** *Demande que l'information sur le système ne puisse être lue que par les personnes autorisées.*
- **Intégrité :** *Demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées.*
- **Non répudiation:** *Permettant de garantir qu'une transaction ne peut être niée.*
- **Authentification:** *Consistant à assurer que seules les personnes autorisées aient accès aux ressources.*

Contrôle d'accès

Il offre 3 services essentiels:

- **Authentification (qui peut se connecter)**
- **Autorisation (ce que les utilisateurs autorisés peuvent faire)**
- **Responsabilisation (identifie ce qu'un utilisateur a fait)**

Types de contrôle d'accès

- Contrôle d'accès centralisé

  **RADIUS (Remote Authentication Dial-In User Service)*

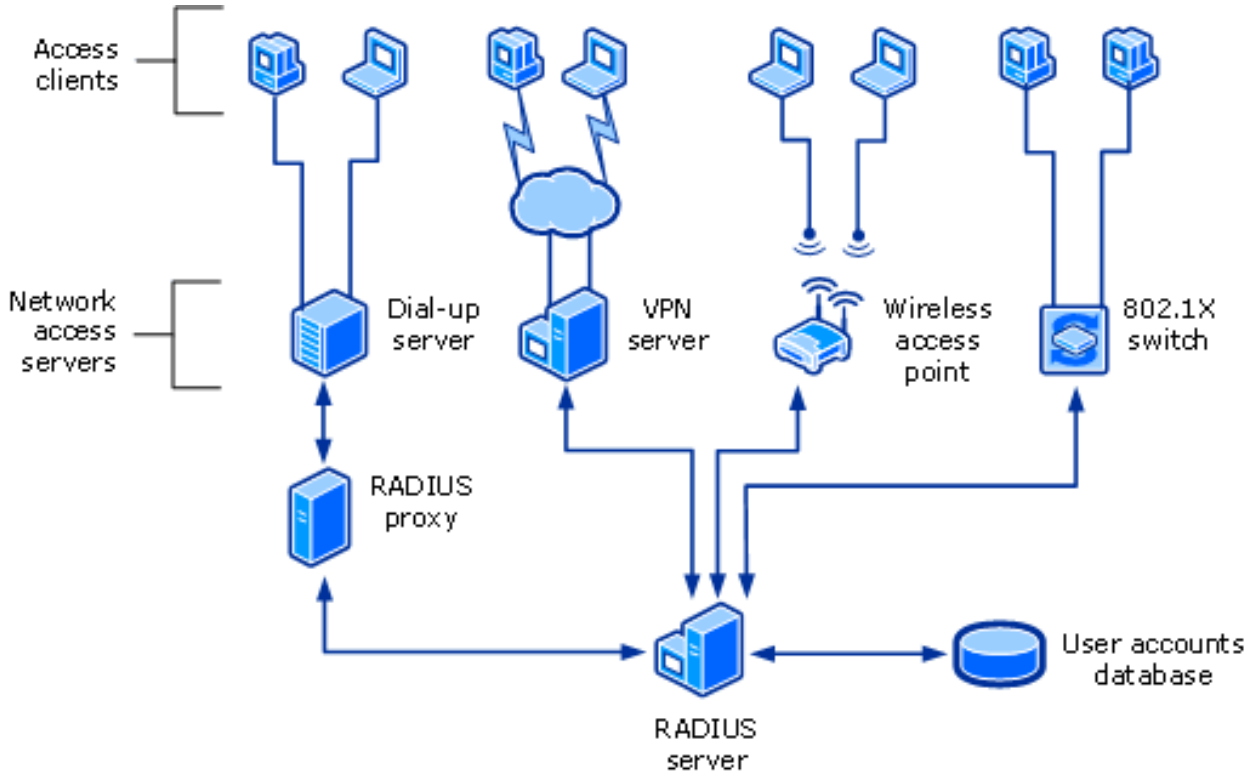
- Contrôle d'accès décentralisé

  *Contrôle de l'accès par les personnes les plus proches de ressources

  *Aucune méthode pour un contrôle cohérent

RADIUS (Remote Authentication Dial-In User Service)

- RADIUS (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification.



Authentification

Un moyen de vérifier ou de prouver l'identité d'un utilisateur

- Le terme «utilisateur» peut désigner:
  - Une personne
  - Application ou processus
  - Machine ou appareil
- Identification avant l'authentification
  - Fournir un nom d'utilisateur pour établir l'identité de l'utilisateur
- Pour prouver l'identité, l'utilisateur doit présenter l'une des informations suivantes:
  - Ce que vous savez (Mots de passe, PIN (Personal Identification Number))
  - Ce que vous avez (Jeton, cartes à puce, codes de passage, RFID)
  - Qui êtes-vous (biométrie comme les empreintes digitales et l'iris scan, signature ou Voix)

Exemples de jetons

eToken

RFID cards

Smart Cards

Fingerprint scanner

Authentification forte (Strong Authentication)

- **Authentification à deux facteurs (Two-factor authentication)**
  - **Mots de passe (quelque chose que vous connaissez)**
  - **Jetons (quelque chose que vous avez)**

  Exemples:

  - Les mots de passe

  - Jetons

  - Des billets

  - PIN

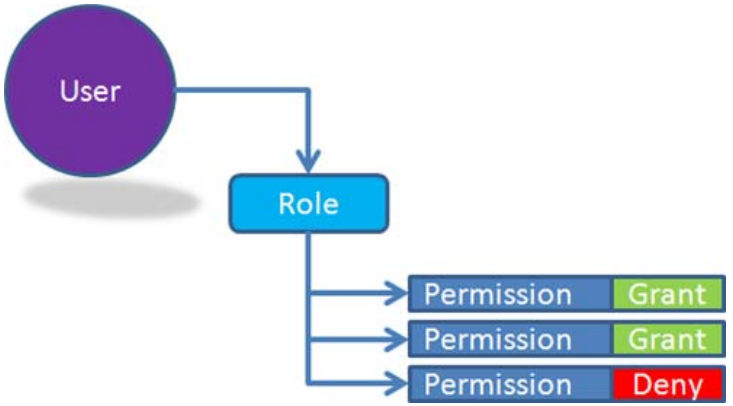
  - Biométrie

  - Certificats

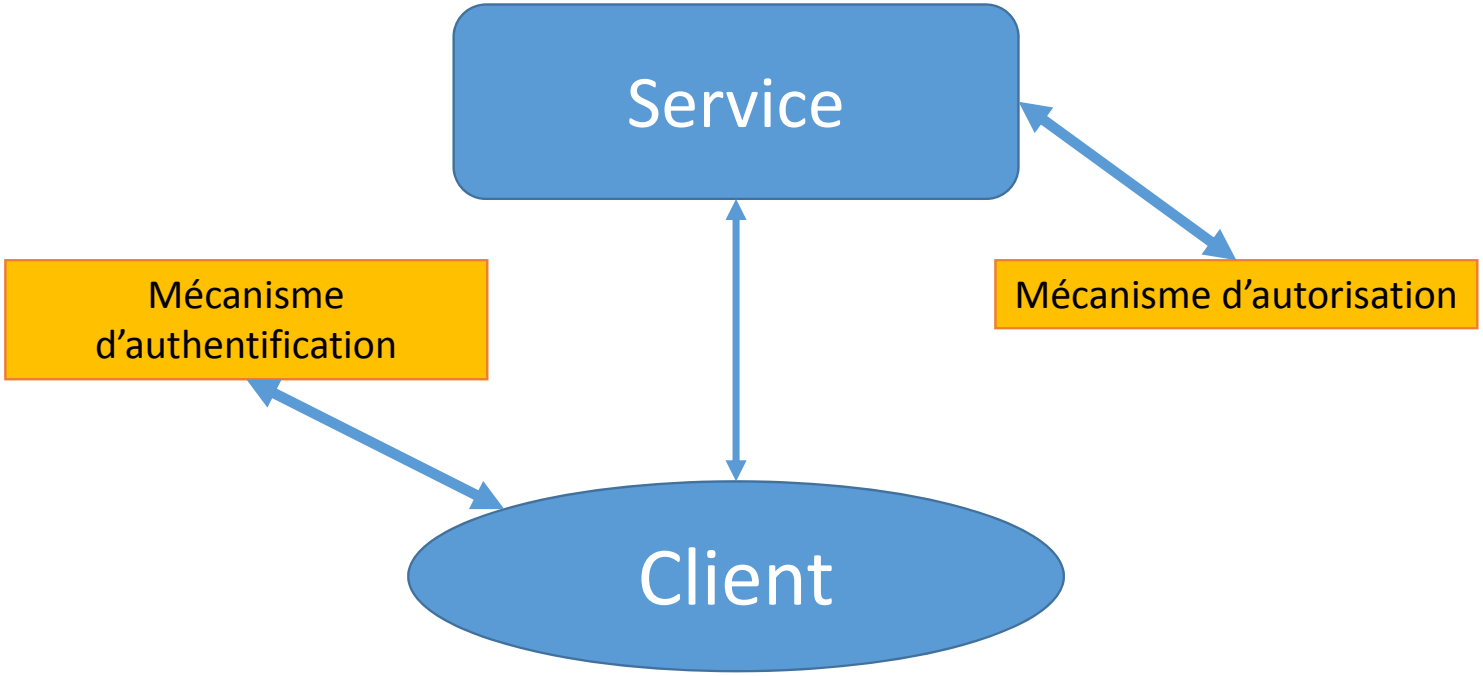
Autorisation

Définit les droits et autorisations de l'utilisateur sur un système

- Généralement effectué après l'authentification de l'utilisateur
- Permet à un utilisateur d'accéder à une ressource particulière et aux actions qu'il est autorisé à effectuer sur cette ressource
- Critères d'accès basés sur le niveau de confiance:
  - Les rôles
  - Groupes
  - Emplacement
  - Temps
  - Type de transaction



Authentification vs. Autorisation



- "Authentification identifie simplement une partie, l'autorisation définit si elles peuvent effectuer une certaine action" - RFC 3552 https://datatracker.ietf.org/doc/rfc3552/

Intégrité

- **Intégrité des données** : La propriété que les données n'ont pas été modifiée d'une manière non autorisée

- **Intégrité du système**: La qualité d'un système lorsqu'il exécute sa fonction prévue de manière intacte, sans manipulation non autorisée

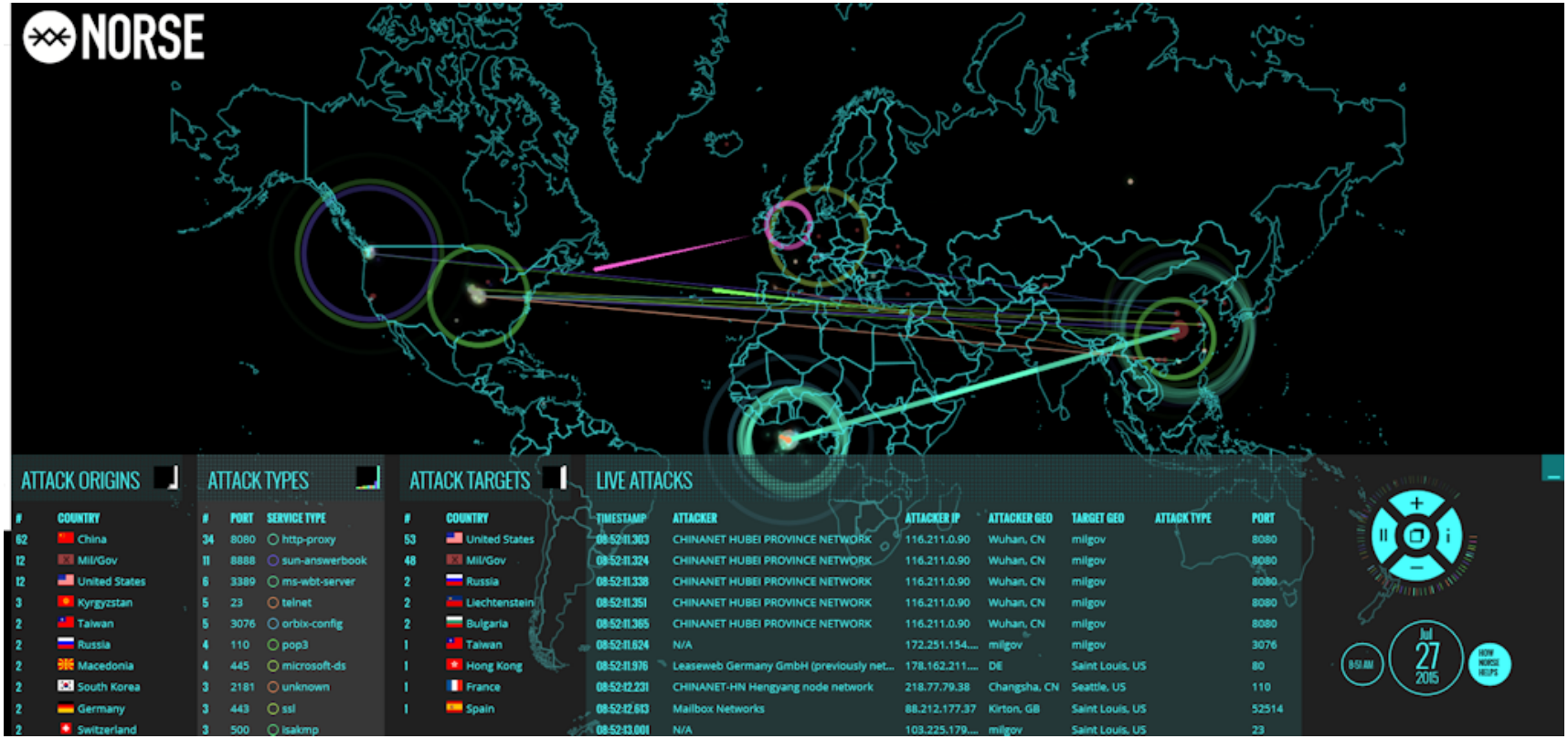
Les menaces informatiques

- 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 ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

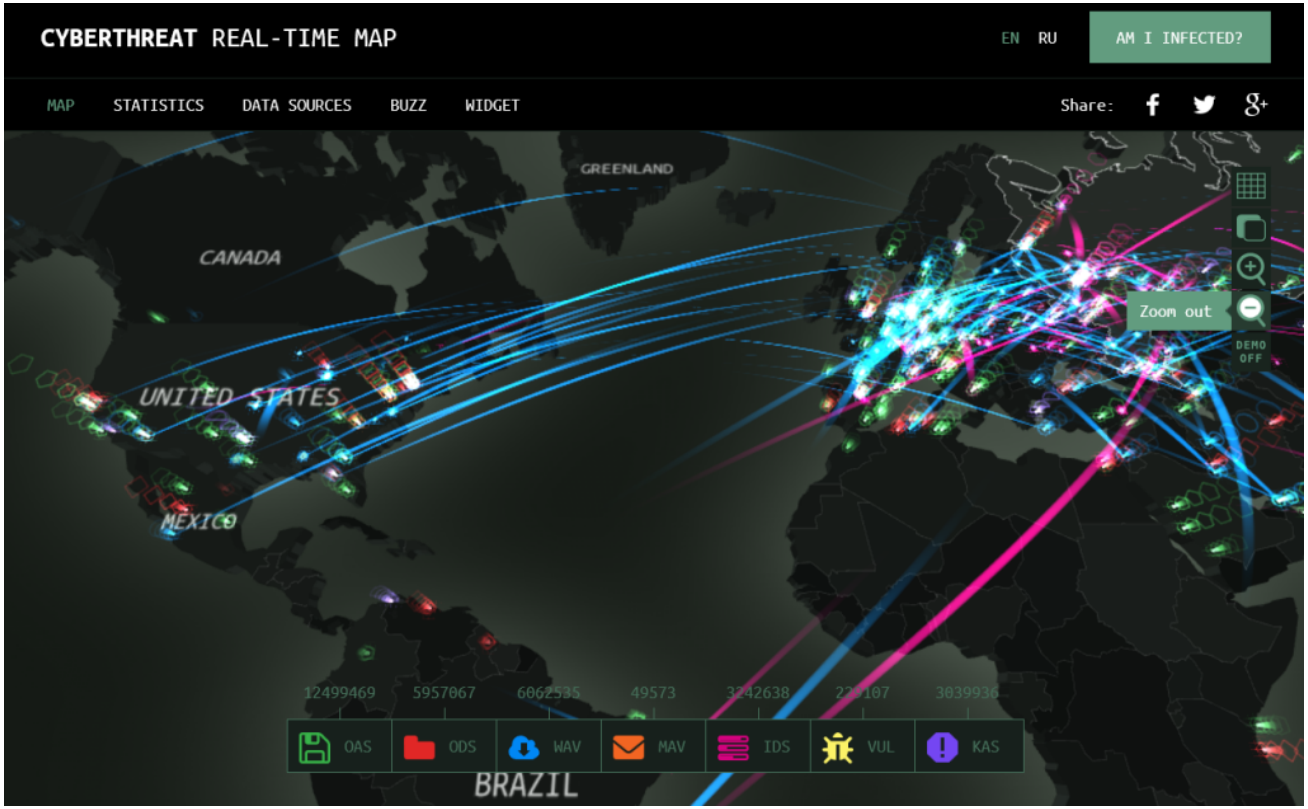
- Afin de détecter ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives.

Les attaques : en temps réel

http://map.norsecorp.com/



https://cybermap.kaspersky.com/



http://threatmap.fortiguard.com/

Type des attaquants : par compétence

- **Script Kiddy**
  - 90% playstation 9% clickomane 1% intelligence
  - utilise ce que font les autres
- **Amateur**
  - Failles connues
  - Failles web
- **Professionnel**
  - En equipe
  - Avec beaucoup de moyens (financiers, techniques, parfois préparatoires)
  - 0days possibles

Type des attaquants : par objectif

- **L'argent**
  - piratage volumétrique
  - cryptolocker "killer application"
- **Hacktiviste**
  - "Terroriste"
  - Anonymous
- **Espions**
  - Etatique
  - Industriel
- **"Petit con"**

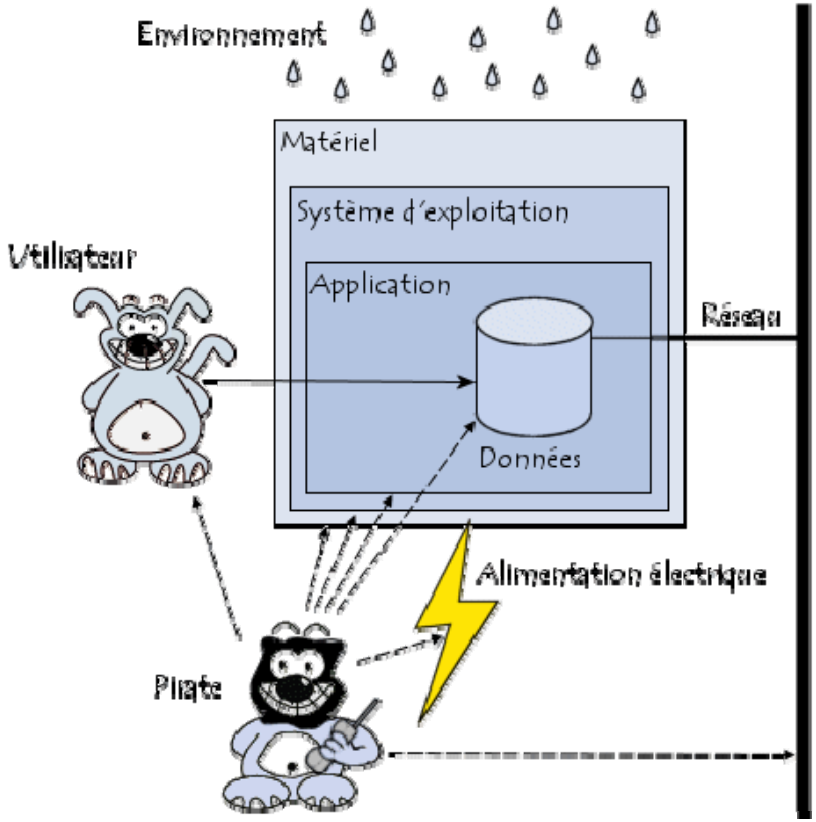
Motivation des attaques

Les motivations des attaques peuvent être de différentes sortes :

- Obtenir un accès au système
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles
- Glaner des informations personnelles sur un utilisateur
- Récupérer des données bancaires ;
- S'informer sur l'organisation (entreprise de l'utilisateur, etc.)
- troubler le bon fonctionnement d'un service
- utiliser le système de l'utilisateur comme « rebond » pour une attaque
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée

Motivation des attaques

- Les systèmes informatiques mettent en oeuvre différentes composantes, allant de l'électricité pour alimenter les machines au logiciel exécuté via le système d'exploitation et utilisant le réseau.
- Les attaques peuvent intervenir à chaque maillon de cette chaîne, pour peu qu'il existe une vulnérabilité exploitable.
- Le schéma à coté rappelle très sommairement les différents niveaux pour lesquels un risque en matière de sécurité existe :



Classification des attaques

- Actif vs. passif

- **Active** consiste à écrire des données sur le réseau. Il est courant de déguiser son adresse et de cacher l'identité de l'expéditeur du traffic.

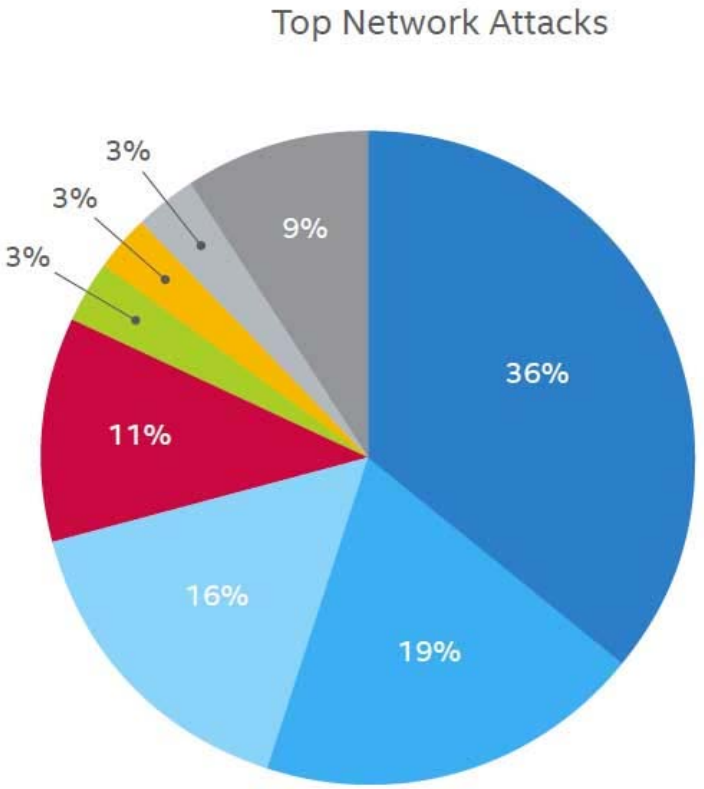
- **Passif** implique uniquement la lecture des données sur le réseau. Son but est la violation de la confidentialité. Ceci est possible si:

• L'attaquant a pris le contrôle d'un hôte sur le chemin de communication entre deux machines victime.

• L'attaquant a compromis l'infrastructure de routage pour organiser le trafic passant par une machine compromise.

Active	Passif
L'attaque DoS Spoofing L'homme au milieu Débordement de tampon Injection SQL	Eavesdropping Port scanning

Les attaques réseaux (Les plus fréquentes)



Les attaques contre navigateurs

L'attaque par force brute est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles.

Une attaque informatique ayant pour but de rendre indisponible un service

Les attaques contre Secure Sockets Layer (SSL) et Transport layer security (TLS)

DNS flood est un type d'attaque de déni de service distribué (DDoS) dans lequel l'attaquant cible un ou plusieurs serveurs DNS (Domain Name System) appartenant à une zone donnée, ce qui tente d'entraver la résolution des enregistrements de ressources de cette zone et de ses sous-zones .

Les pirates utilisent les programmes de backdoor pour accéder au réseau de la victime.

L’attaque par rebond

- Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les attaques par rebond (par opposition aux attaques directes), consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui (telle que son adresse IP) et dans le but d'utiliser les ressources de la machine servant de rebond.

- Cela montre l'intérêt de protéger son réseau ou son ordinateur personnel, il est possible de se retrouver « complice » d'une attaque et en cas de plainte de la victime, la première personne interrogée sera le propriétaire de la machine ayant servi de rebond.
- Avec le développement des réseaux sans fils, ce type de scénario risque de devenir de plus en plus courant car lorsque le réseau sans fil est mal sécurisé, un pirate situé à proximité peut l'utiliser pour lancer des attaques !

Les attaques de l'accès physique

Il s'agit d'un cas où l'attaquant à accès aux locaux, éventuellement même aux machines :

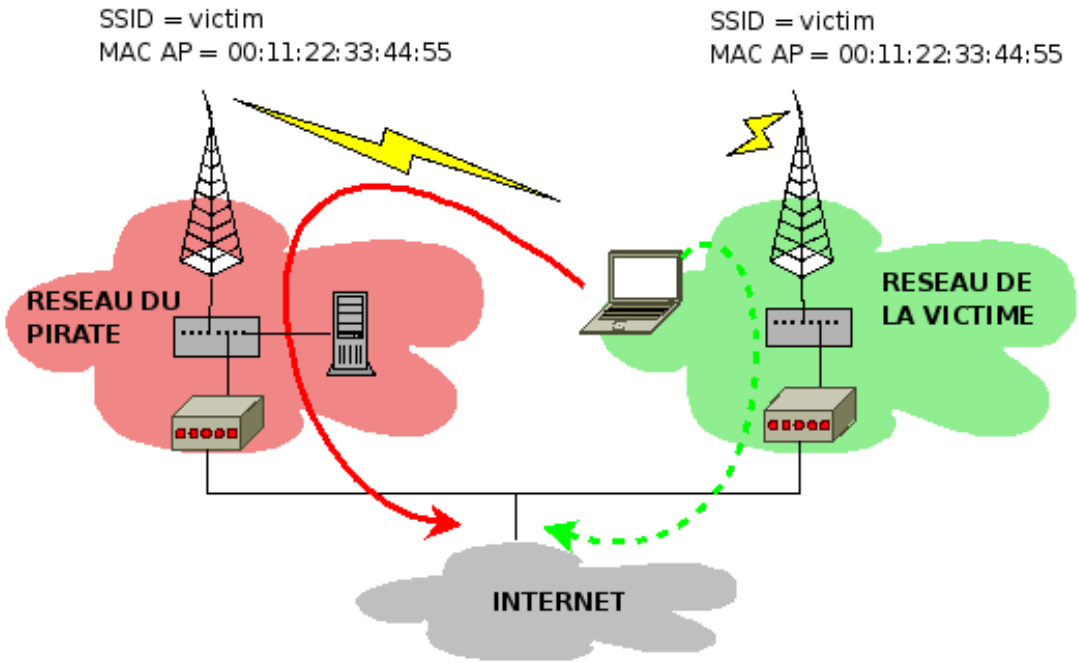
- Coupure de l'électricité
- Extinction manuelle de l'ordinateur
- Ouverture du boîtier de l'ordinateur et vol de disque dur
- Ecoute du trafic sur le réseau

Les attaques de communications (1)

- Vol de session (session hijacking)
- Usurpation d'identité
- Détournement ou altération de messages

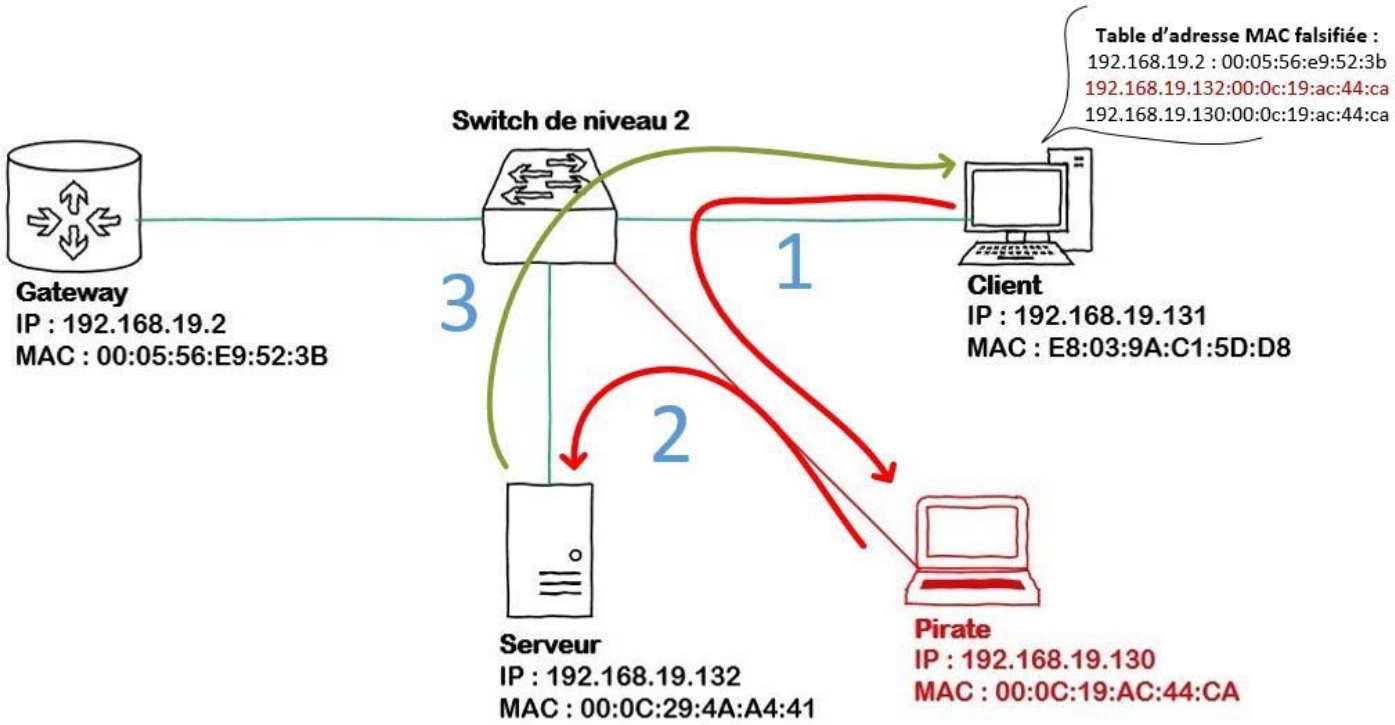
Les attaques de communications (2)

- Vol de session (session hijacking)



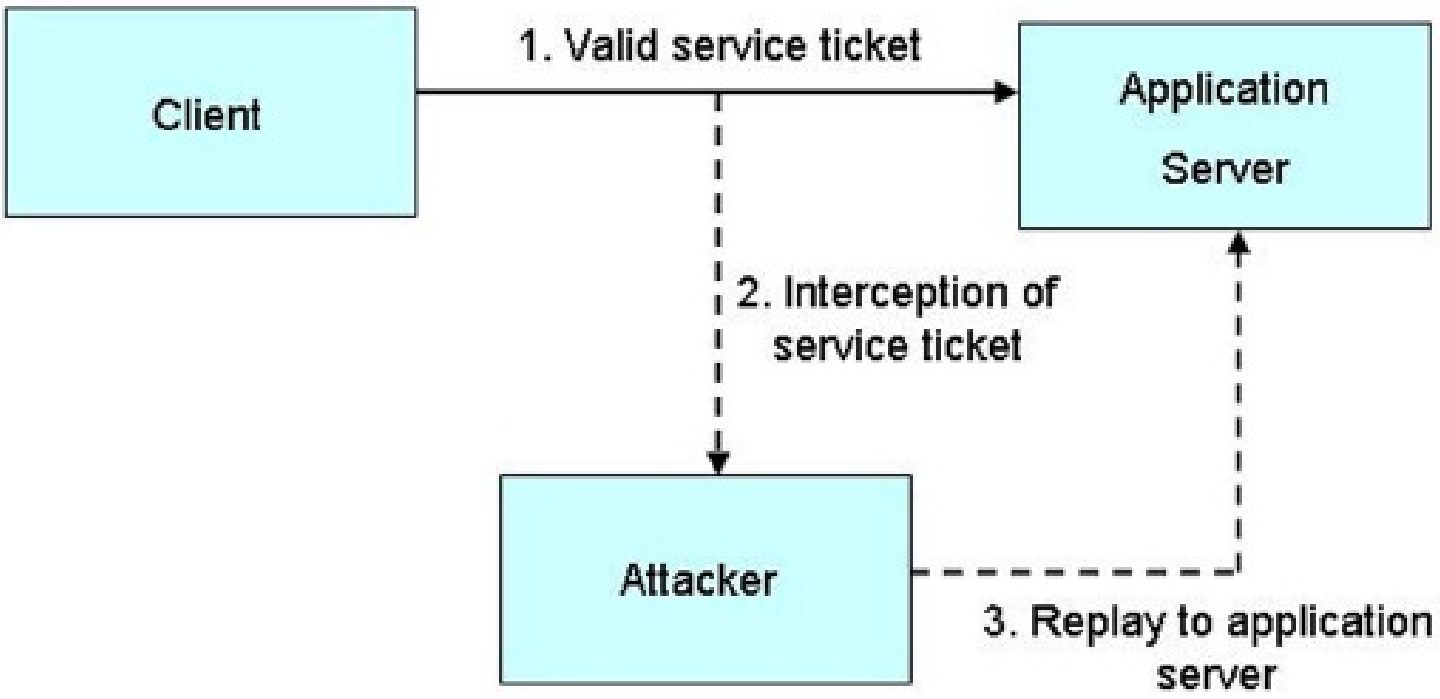
Les attaques de communications (3)

- Usurpation d'identité



Les attaques de communications (4)

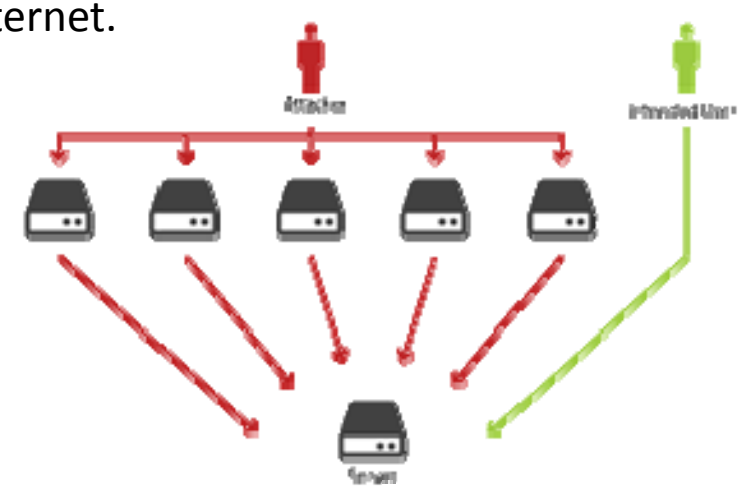
- Détournement ou altération de messages



Les attaques DoS

Une attaque par déni de service (en anglais, denial of service attack [DoS] ou distributed denial of service attack [DDoS]) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il peut s'agir de :

- l'inondation d'un réseau afin d'empêcher son fonctionnement ;
- la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- l'obstruction d'accès à un service à une personne en particulier ;
- également le fait d'envoyer des milliards d'octets à une box internet.



Historique sur les attaques DoS

- La première attaque DDoS officielle a eu lieu en août 1999 : un outil appelé « Trinoo DDO » a été déployé dans au moins 227 systèmes, dont 114 étaient sur Internet, pour inonder les serveurs de l'université du Minnesota. À la suite de cette attaque, l'accès internet de l'université est resté bloqué pendant plus de deux jours.
- La première attaque DDoS médiatisée dans la presse grand public a eu lieu en février 2000, causée par Michael Calce, mieux connu sous le nom de Mafiaboy. Le 7 février, Yahoo! a été victime d'une attaque DDoS qui a rendu son portail Internet inaccessible pendant trois heures. Le 8 février, Amazon.com, Buy.com, CNN et eBay ont été touchés par des attaques DDoS qui ont provoqué soit l'arrêt soit un fort ralentissement de leur fonctionnement. Le 9 février, E-Trade et ZDNet ont à leur tour été victimes d'attaques DDoS. (il n'était âgé que de 15 ans)

- …. Aujourdhui, c'est par tout…

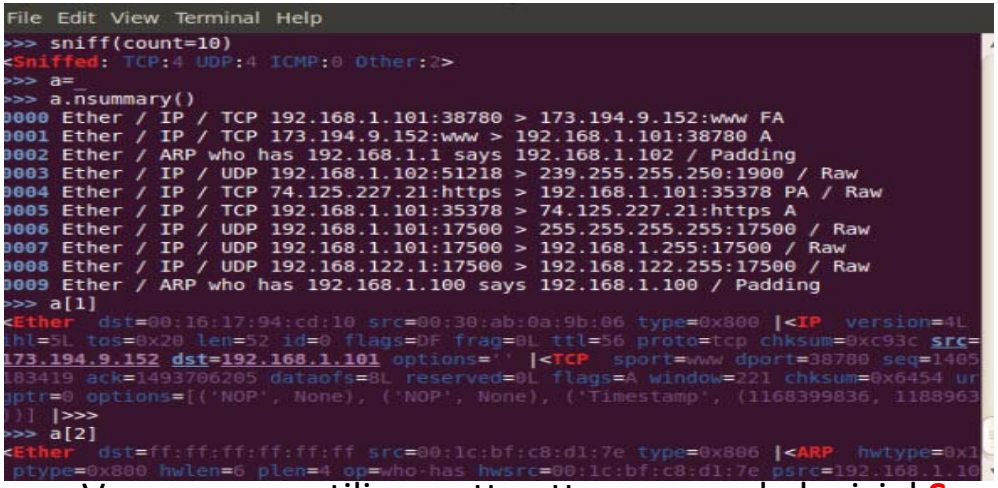
L’attaque de collisions

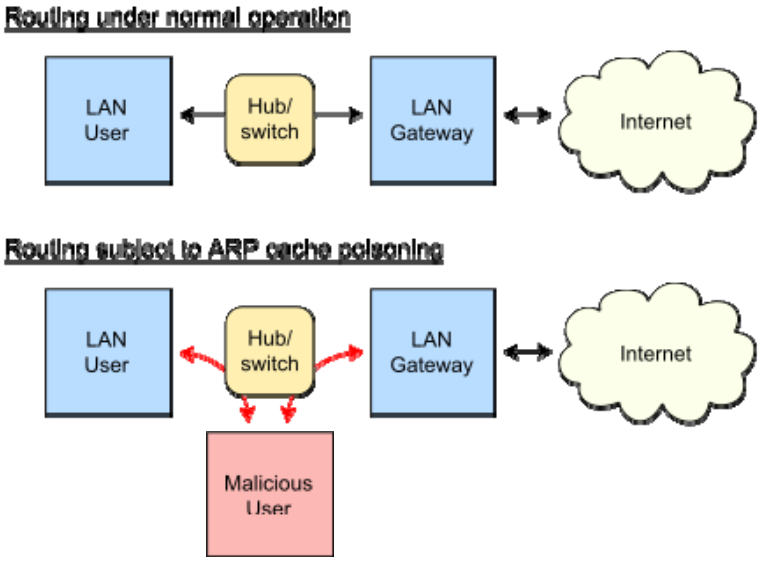
- Une attaque de collisions est une attaque sur une fonction de hachage cryptographique qui tente de trouver deux entrées de cette fonction qui produisent le même résultat (appelé valeur de hachage), c'est-à-dire qui résultent en une collision.
- Il existe deux types principaux d'attaques de collisions :
    - L'attaque de collisions classique : cette attaque consiste à trouver deux messages m1 et m2 différents, tels que hachage (m1) = hachage (m2) ;
    - L'attaque de collisions avec préfixes choisis : étant donné deux préfixes différents P1 et P2, cette attaque consiste à trouver deux suffixes S1 et S2 tels que hachage (P1 ‖ S1) = hachage (P2 ‖ S2) (où ‖ est l'opération de concaténation).

L'attaque nécessitait environ 2^{50} évaluations de la fonction MD5

L’attaque ARP spoofing

- Une technique utilisée pour attaquer tout réseau local utilisant le protocole de résolution d'adresse ARP, les cas les plus répandus étant les réseaux Ethernet et Wi-Fi. Cette technique permet à l'attaquant de détourner des flux de communications transitant entre une machine cible et une passerelle : routeur, box, etc. L'attaquant peut ensuite écouter, modifier ou encore bloquer les paquets réseaux.





Remarque : Vous pouvez utiliser cette attaque avec le logiciel **Scapy**

Un logiciel libre de manipulation de paquets réseau écrit en python

http://www.secdev.org/projects/scapy/

Liste des sujets (Pour les exposés)

1. HTTPS	21. SHA-256
2. TLS/SSL	22. Arbre de Merkle
3. SET (Secure Electronic Transaction)	23. Bcrypt
4. YesCard	24. Message Digest 6 (MD6)
5. OpenSSL	
6. CrypTool	
7. Freenet	
8. L'attaque par rejeu (Replay attack)	
9. L'attaque de l'homme du milieu	
10. L'attaque trou de ver (Wormhole attack)	
11. SQL Injection	
12. RC5 (chiffrement)	
13. Data Encryption Standard (DES)	
14. Advanced Encryption Standard (AES)	
15. Le chiffrement RSA	
16. Digital Signature Algorithm (DSA)	
17. Système de détection d'intrusion (IDS)	
18. Systèmes de prévention d'intrusion (IPS)	
19. L'échange de clés Diffie-Hellman	
20. Message Digest 5 (MD5)	

Références

- Pieprzyk, J., Hardjono, T., & Seberry, J. (2013). *Fundamentals of computer security*. Springer Science & Business Media.

- Goodrich, M., & Tamassia, R. (2010). *Introduction to computer security*. Addison-Wesley Publishing Company.

- Peltier, T. R. (2013). *Information security fundamentals*. CRC Press.

- Easttom II, W. C. (2016). *Computer security fundamentals*. Pearson IT Certification.