# Sécurité des Réseaux


P. Laurençot

# Plan général

1. **Quelques rappels**
   - Sur Internet /réseau
   - Sur les équipements
   - Sur le vocabulaire et les types d'attaque

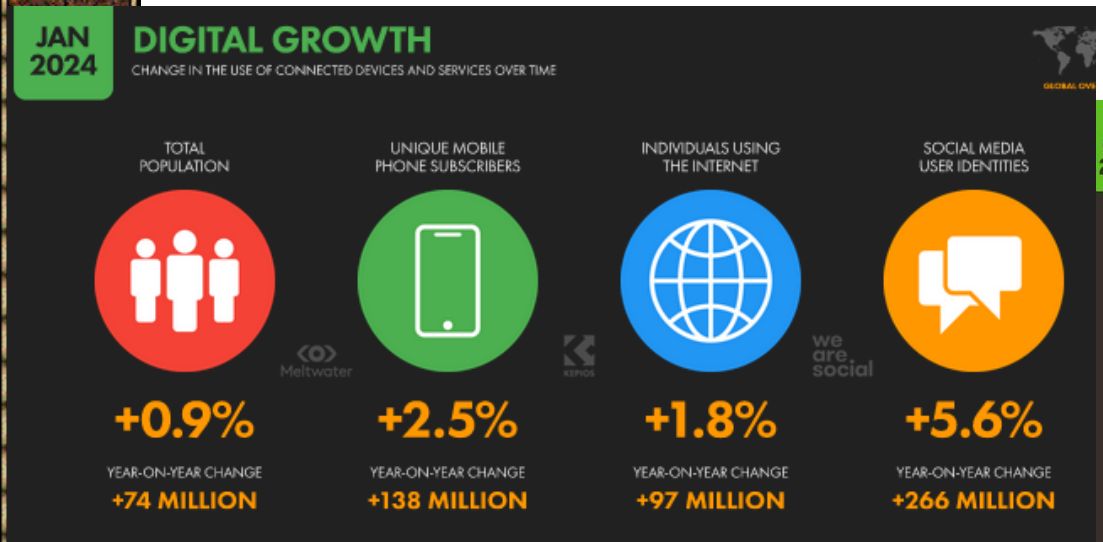
2. **Sécurité des accès**
   - Filtrage
   - Utilisation de parefeu

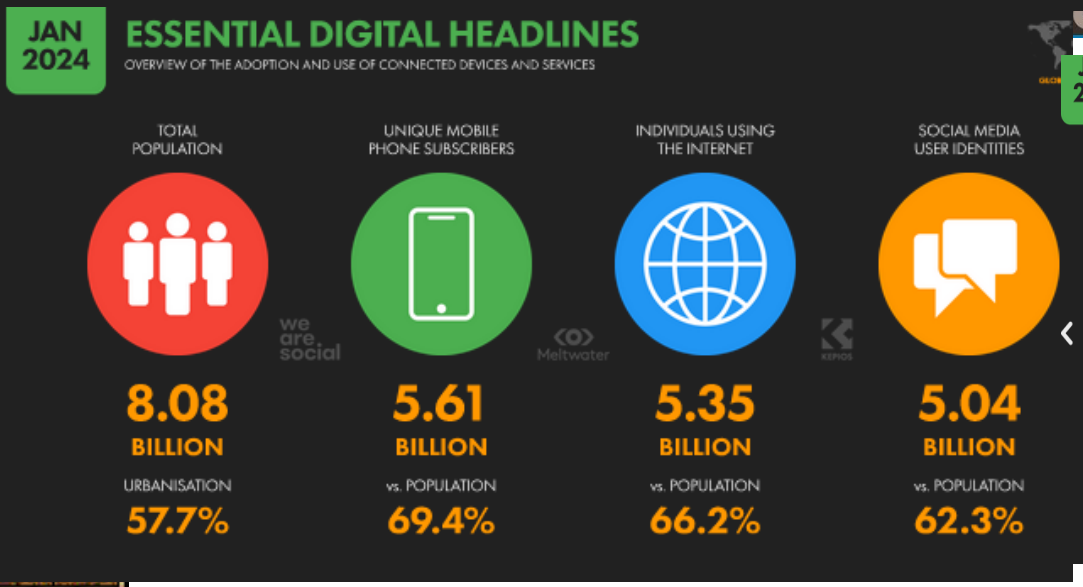
3. **Sécurité des échanges**
   - PKI
   - IPsec

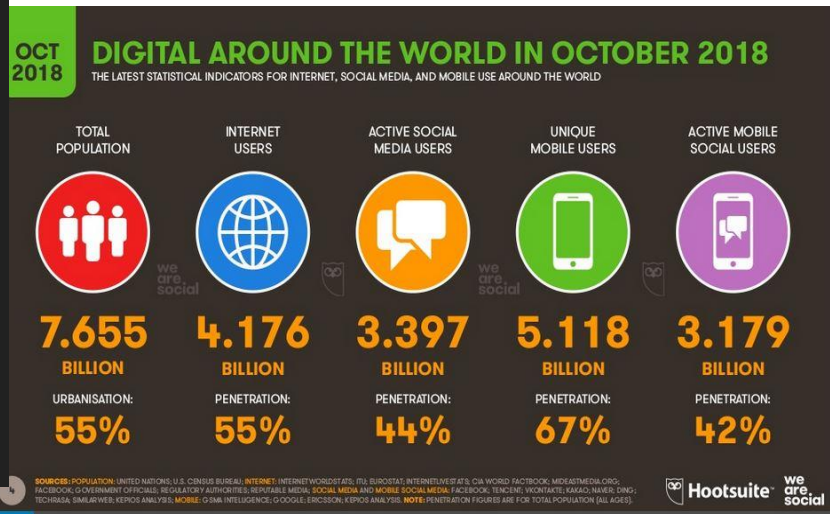
# Introduction

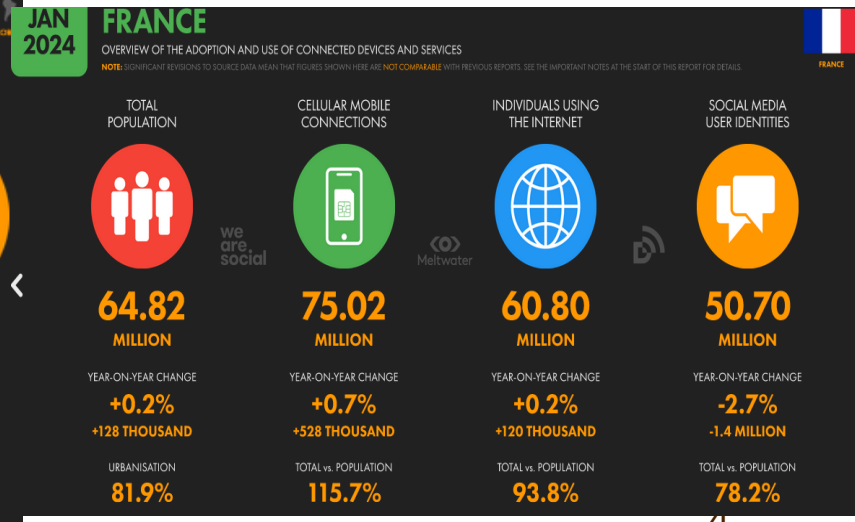
# Quelques chiffres sur Internet (1)

Utilisateurs internet

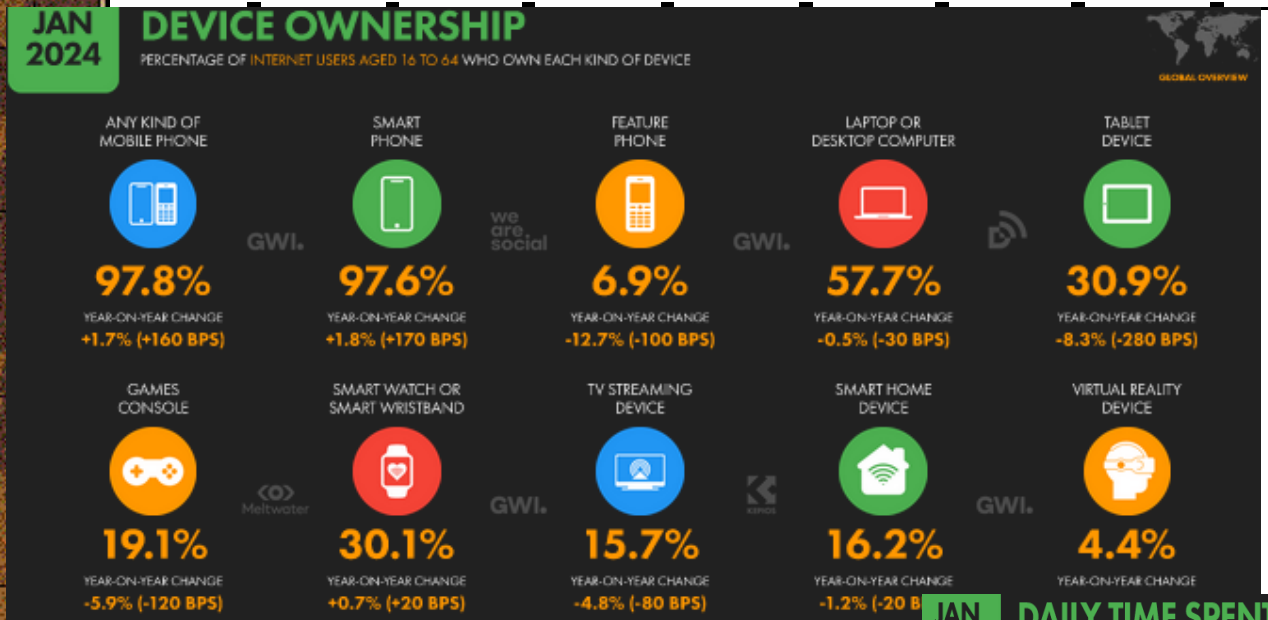


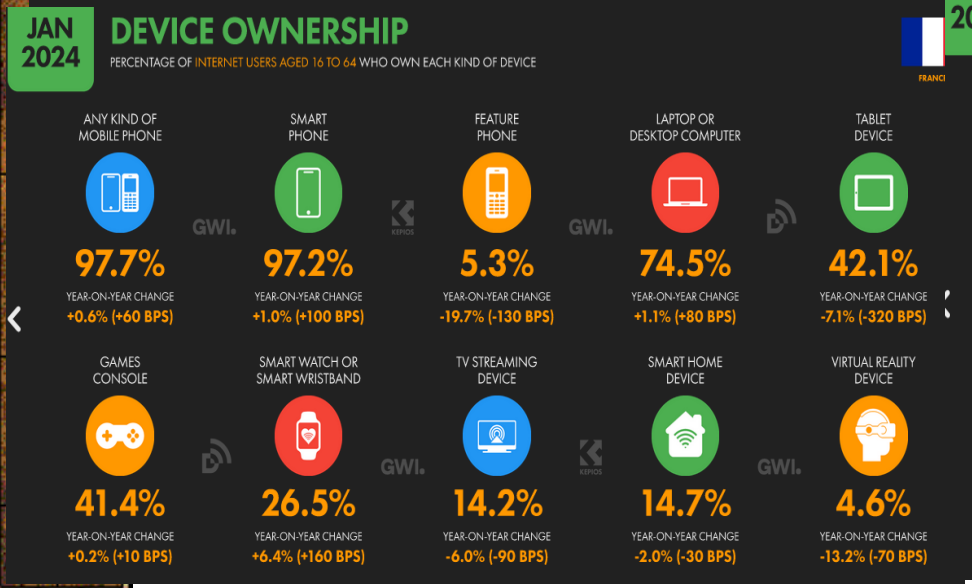



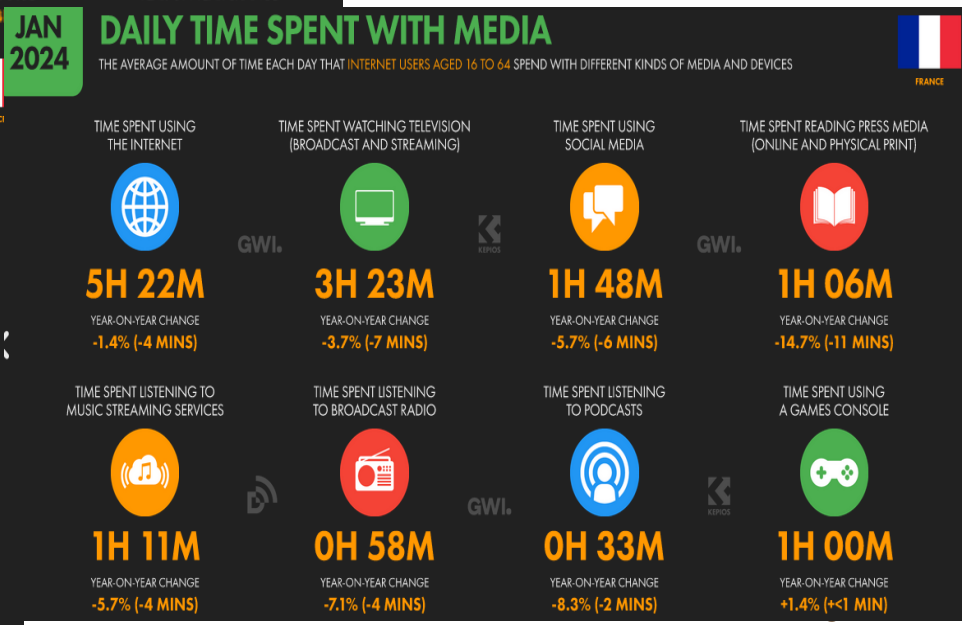



# Quelques chiffres sur Internet (2)

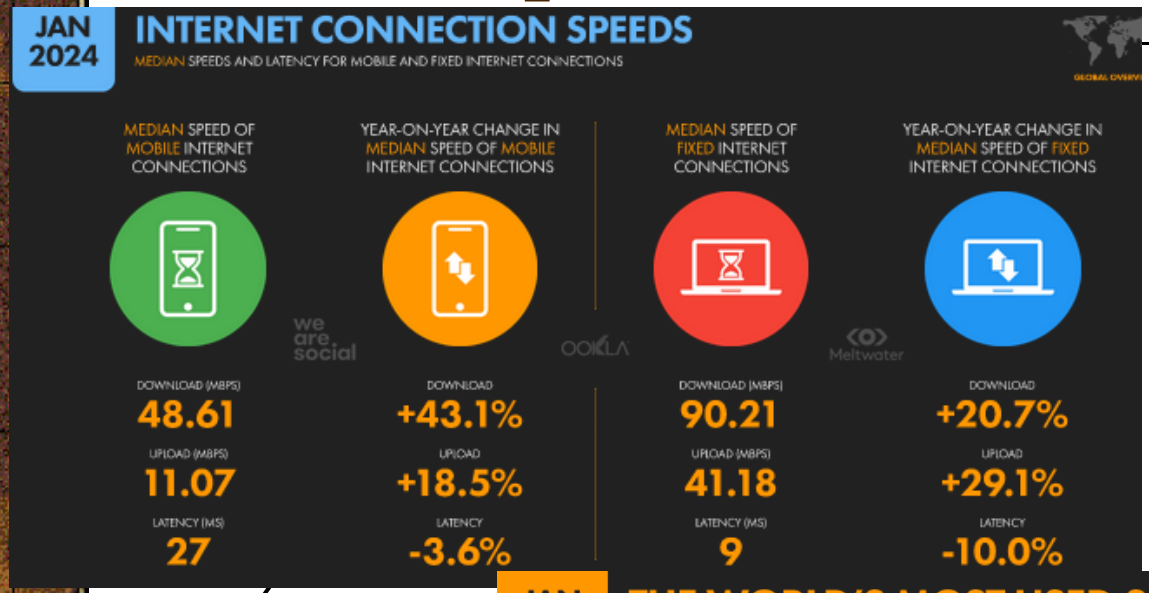



Différents équipements pour aller sur internet



# Quelques chiffres sur Internet (3)




Connexion de plus en plus rapide

Les réseaux sociaux sont très actifs (moyenne 2h23), inscrit sur 6 plateformes différentes

France :

79,66 Mbps mobile

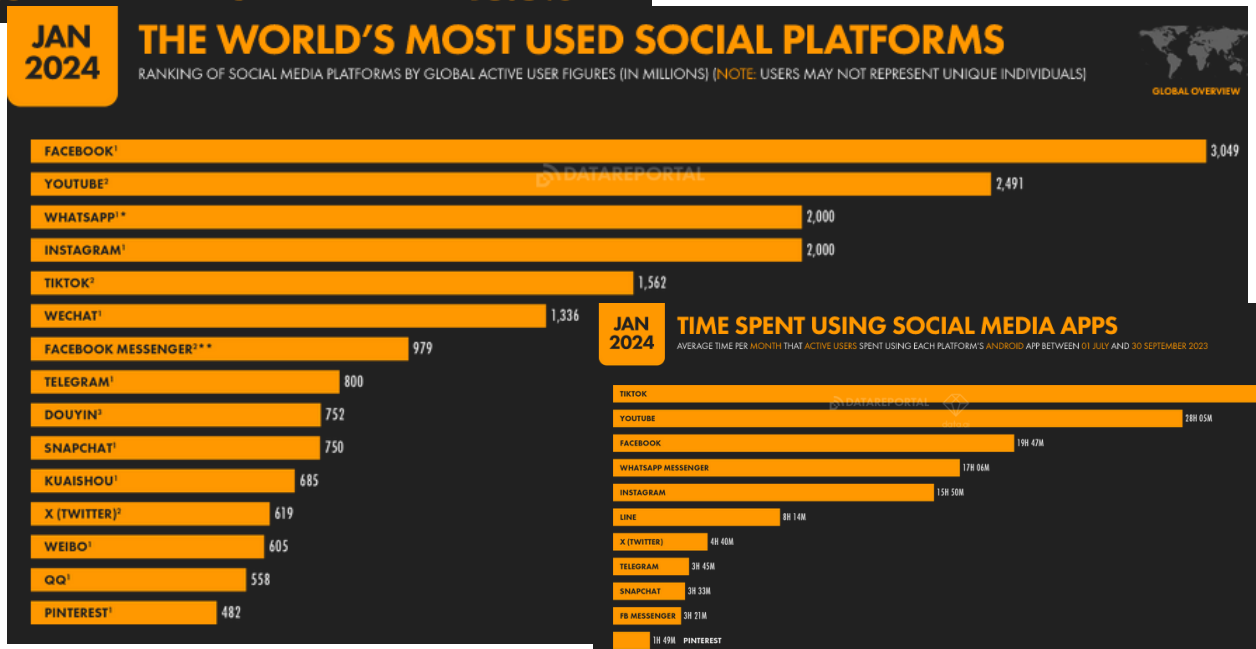
207,41 Mbps fixe

U.A.E : 324 Mbps

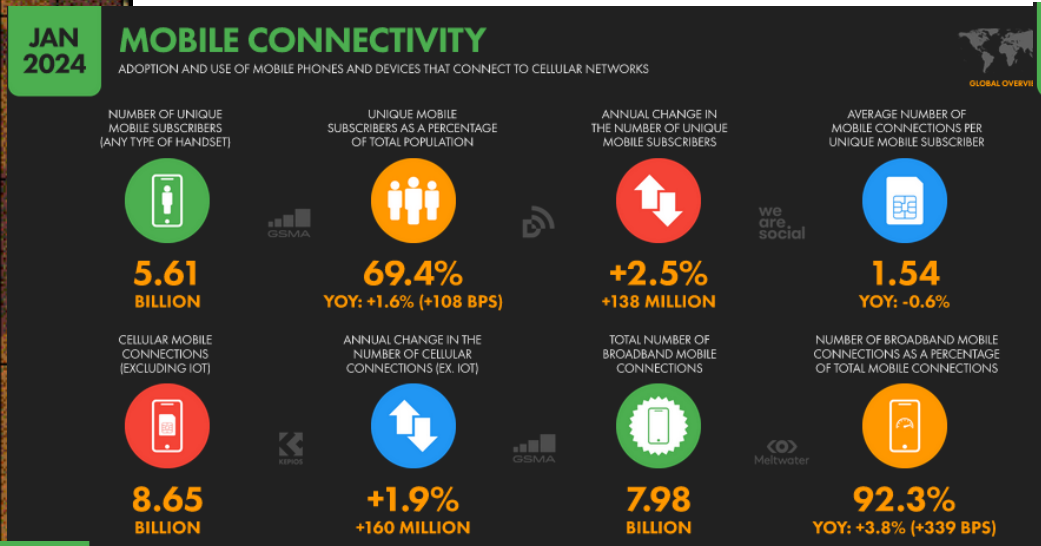
Singapore : 263 Mbps

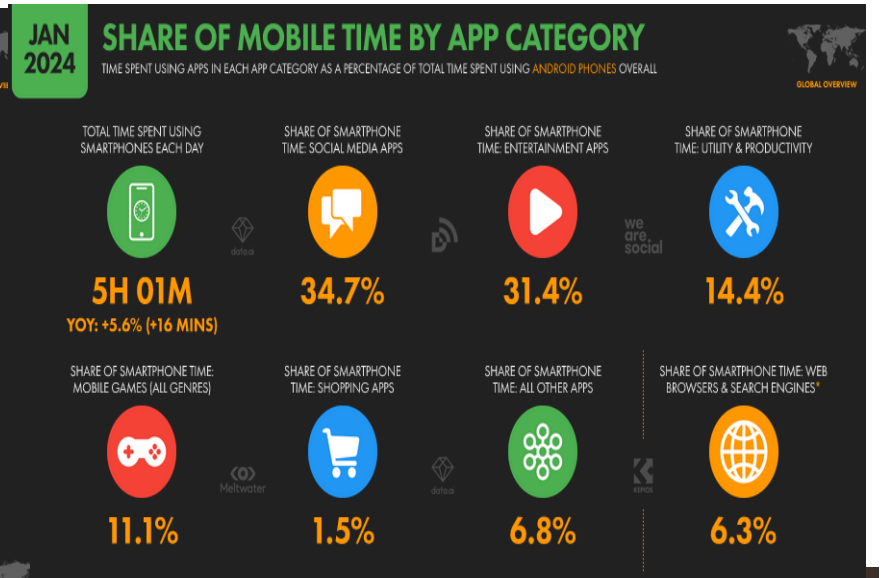
Cuba : 3,9 Mbps

Cuba : 2,11 Mbps

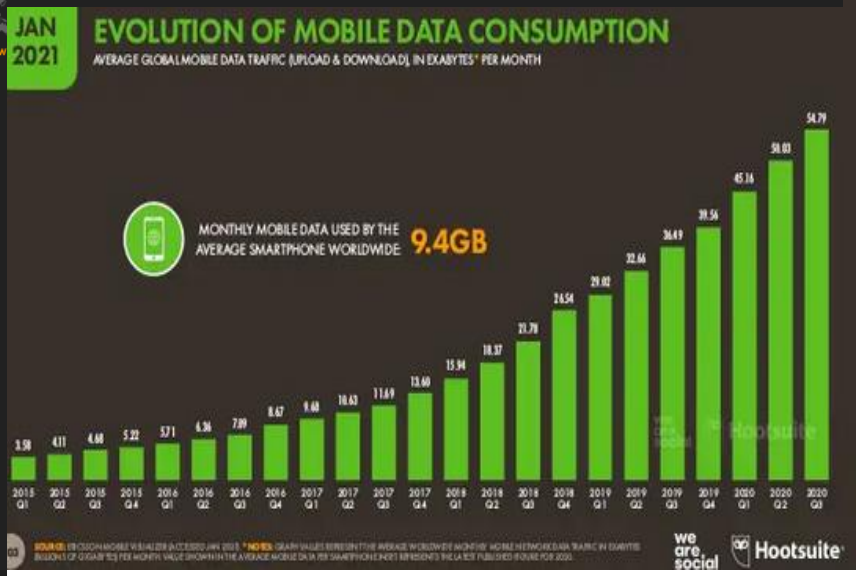


# Quelques chiffres sur Internet (4)

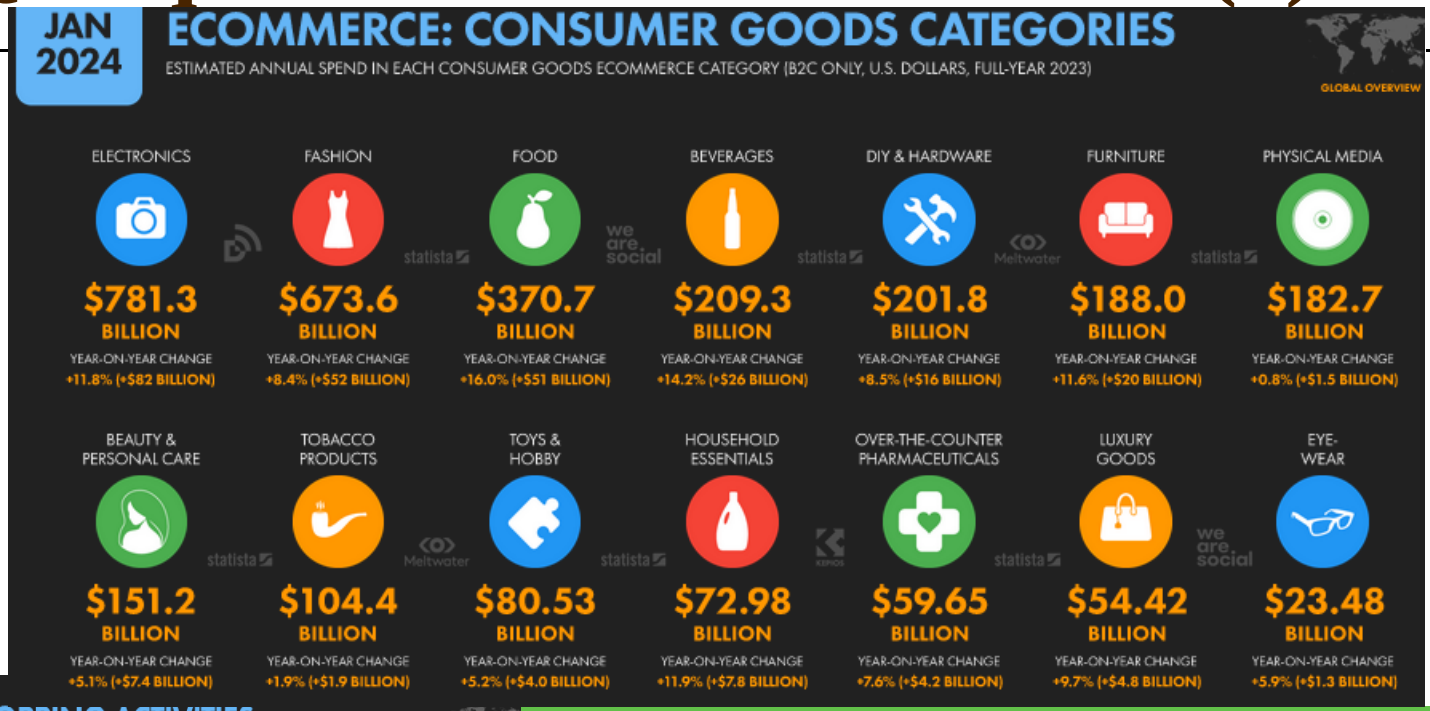






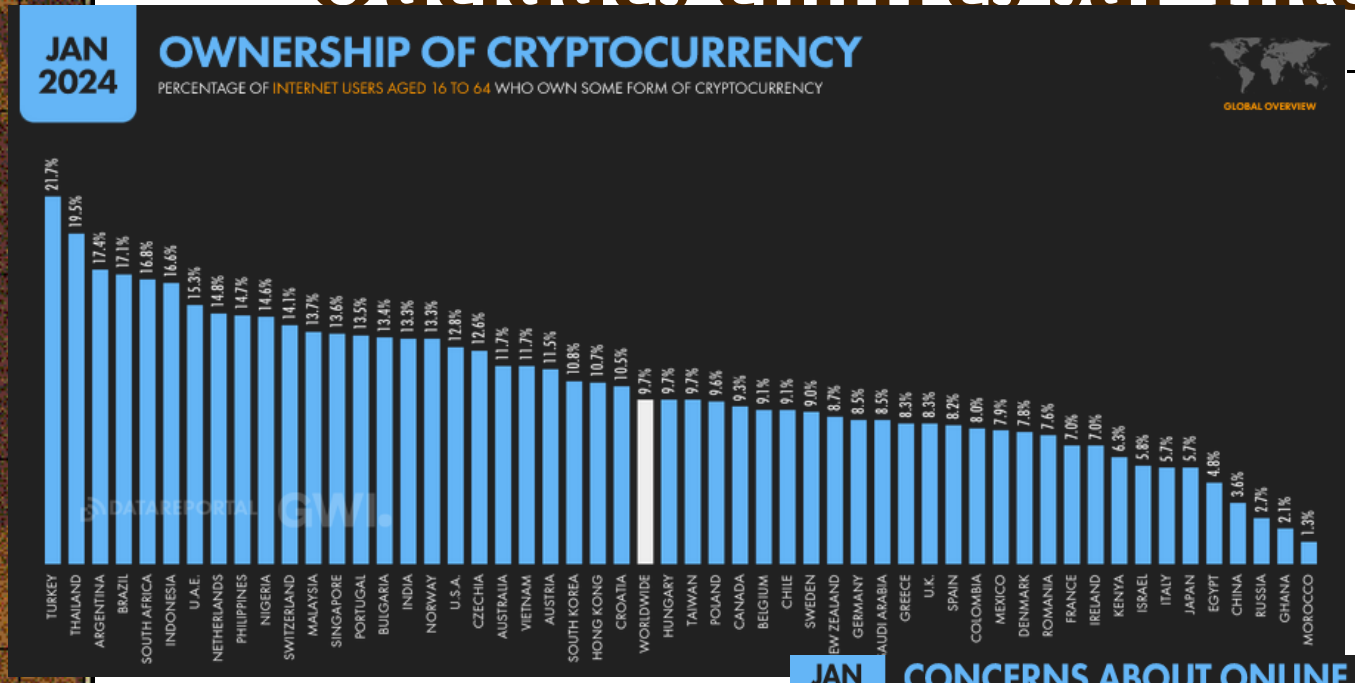
# Quelques chiffres sur Internet (5)

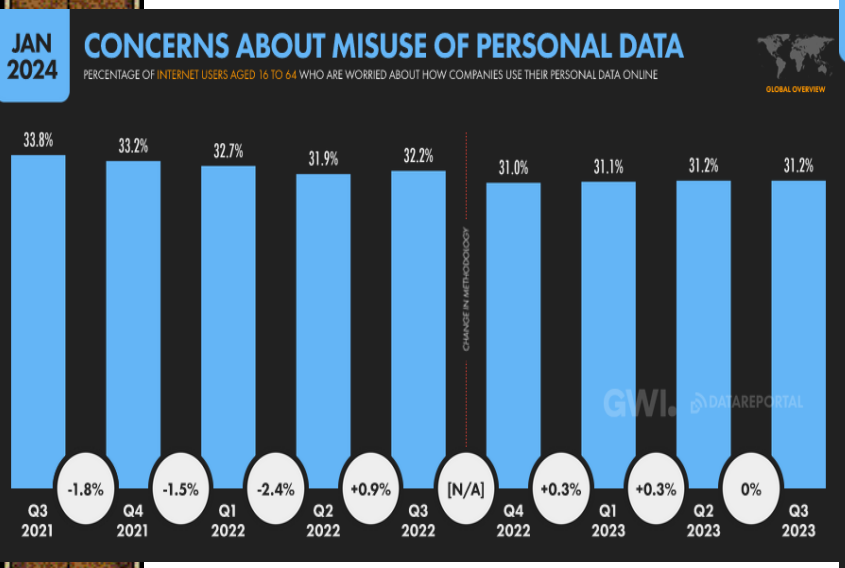


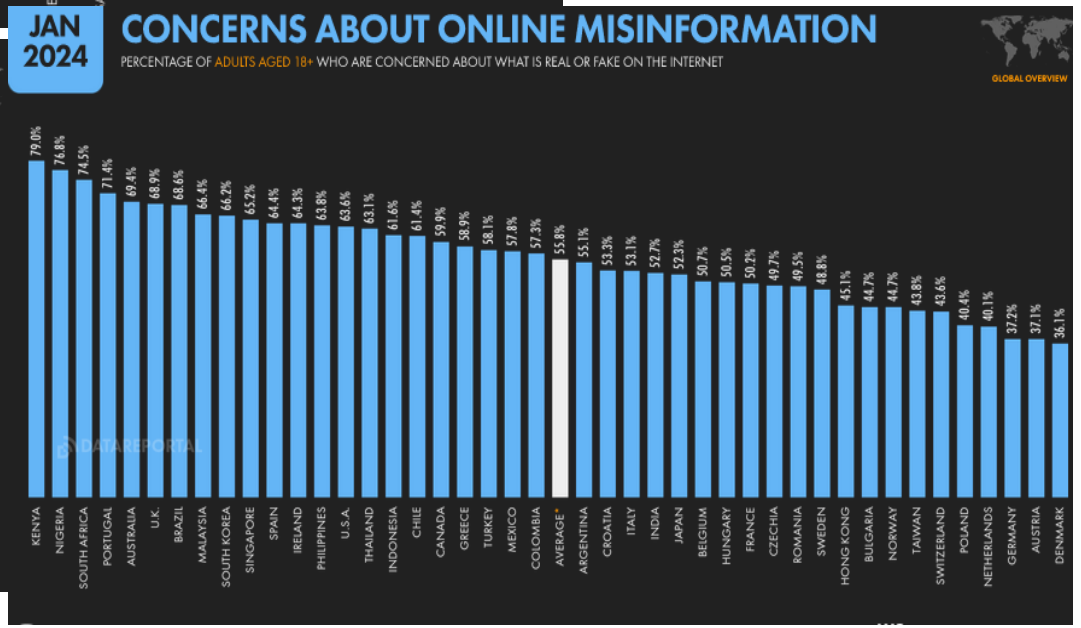

©wearesocial.comv


1. PROTÉGEZ VOS COMPTES AVEC DES MOTS DE PASSE ROBUSTES
2. SAUVEGARDEZ VOS DONNÉES RÉGULIÈREMENT
3. FAITES SANS TARDER LES MISES À JOUR DE SÉCURITÉ SUR TOUS VOS APPAREILS
4. UTILISEZ UN ANTIVIRUS
5. SOYEZ PRUDENTS LORS DE VOS ACHATS EN LIGNE
6. MÉFIEZ-VOUS DES MESSAGES SUSPECTS
7. APPRENEZ À MAÎTRISER VOS RÉSEAUX SOCIAUX

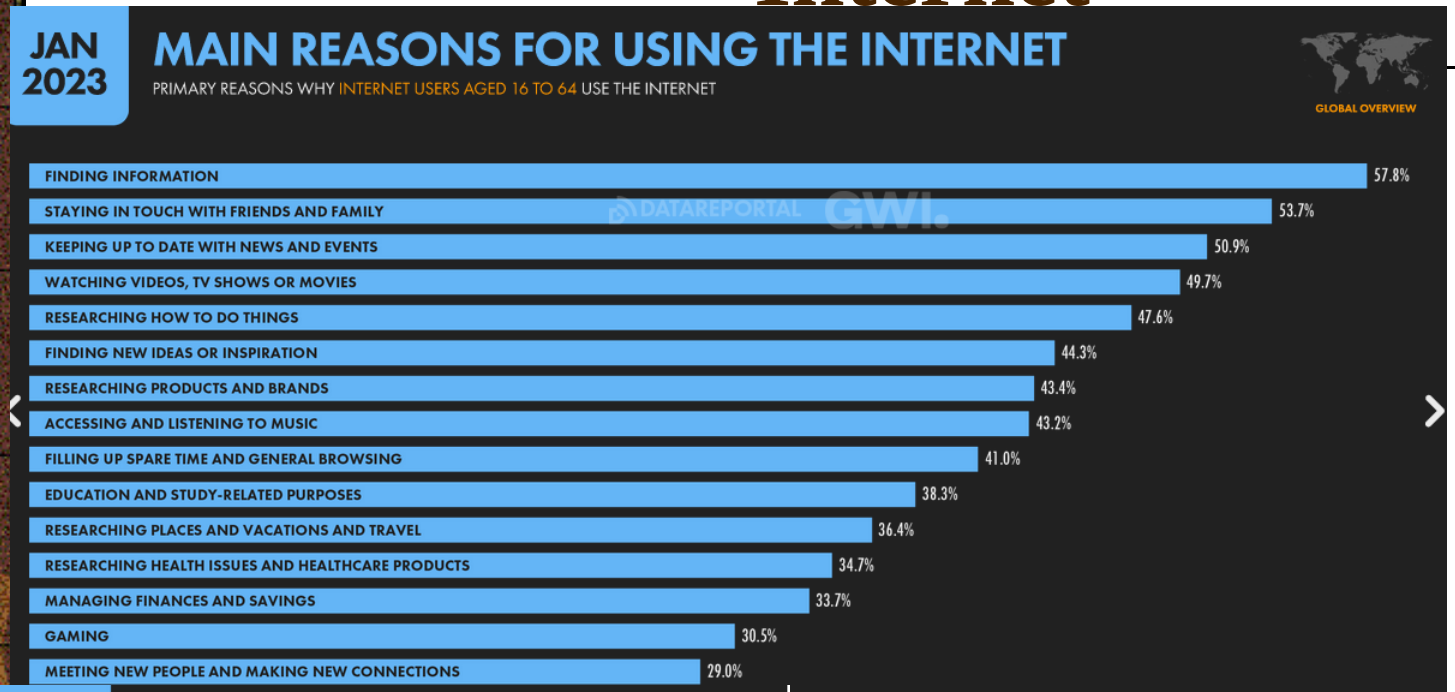
# Quelques chiffres sur Internet (6)

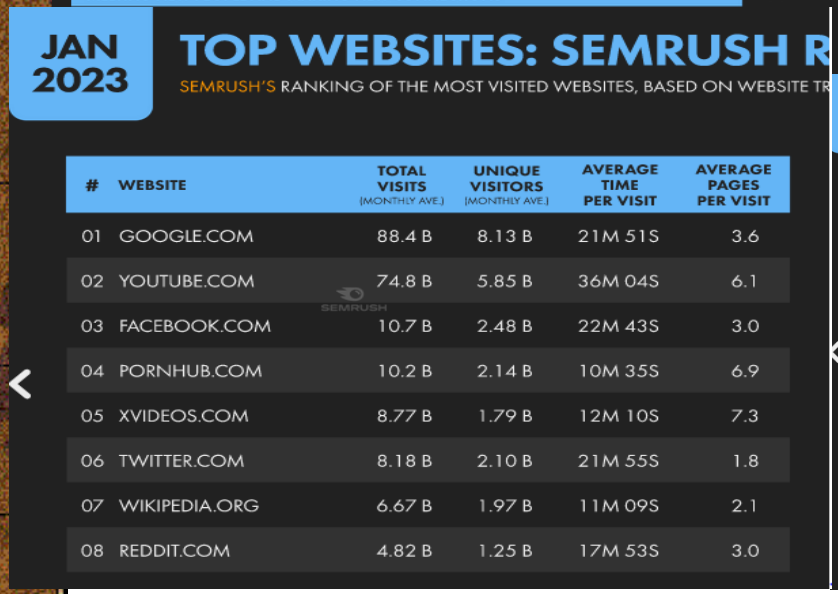


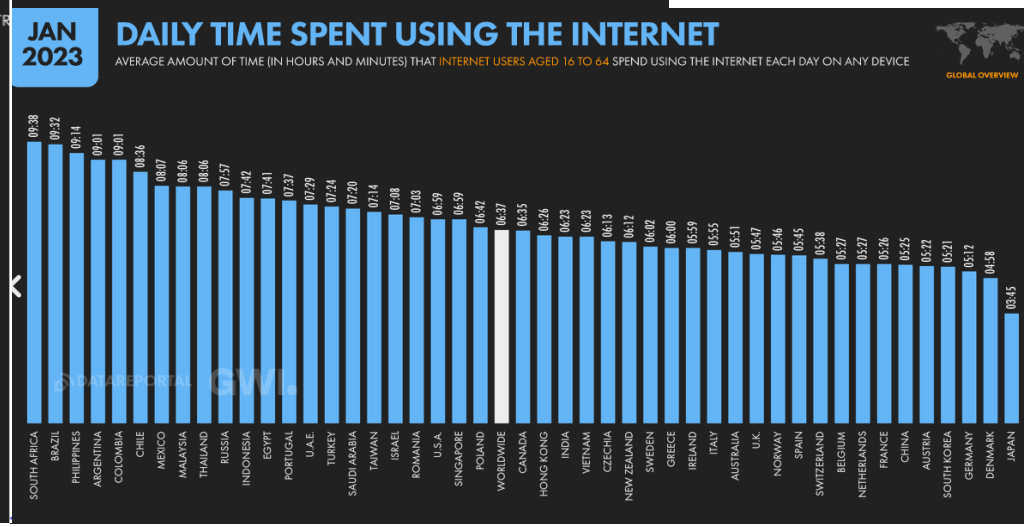



# Internet




| # | WEBSITE | TOTAL VISITS (MONTHLY AVE.) | UNIQUE VISITORS (MONTHLY AVE.) | AVERAGE TIME PER VISIT | AVERAGE PAGES PER VISIT |
|---|---|---|---|---|---|
| 01 | GOOGLE.COM | 88.4 B | 8.13 B | 21M 51S | 3.6 |
| 02 | YOUTUBE.COM | 74.8 B | 5.85 B | 36M 04S | 6.1 |
| 03 | FACEBOOK.COM | 10.7 B | 2.48 B | 22M 43S | 3.0 |
| 04 | PORNHUB.COM | 10.2 B | 2.14 B | 10M 35S | 6.9 |
| 05 | XVIDEOS.COM | 8.77 B | 1.79 B | 12M 10S | 7.3 |
| 06 | TWITTER.COM | 8.18 B | 2.10 B | 21M 55S | 1.8 |
| 07 | WIKIPEDIA.ORG | 6.67 B | 1.97 B | 11M 09S | 2.1 |
| 08 | REDDIT.COM | 4.82 B | 1.25 B | 17M 53S | 3.0 |



# Des statistiques !!

- En moyenne, il faut **6 mois** à une entreprise pour détecter une violation de ses données ( 50000 euros, coût médian d'une cyberattaque)
- La plupart des domaines de nom malveillants ( site ressemblant à un site connu), environs 60%, sont associés à des campagnes de spam.
- Les attaques de ransomware se produisent tous **les 10 secondes**.
- 54% des entreprises françaises attaquées en 2021.
- 41% des entreprises ont plus de 1 000 fichiers sensibles, y compris les numéros de carte de crédit et les dossiers médicaux, laissés sans protection.
- 94% de tous les logiciels malveillants est livré par e-mail.
- 65% des entreprises ont des utilisateurs qui ne modifient jamais leurs mots de passe.
- 69% des entreprises ne pensent pas que leur logiciel anti-virus puisse bloquer les menaces qu'elles détectent.
- 50% des structures victimes portent plainte

# OWASP

Open Web Application Security project

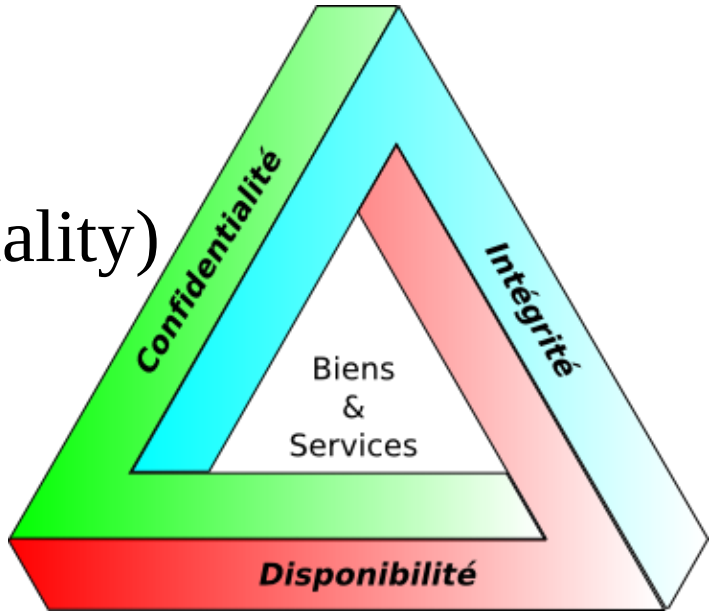
- Authentification brisée - Broken access control
- Exposition de données sensibles (crytographic failure)
- Injection SQL (y compris XSS)
- Insecure Design
- Security misconfigurations
- Using components with known vulnerabilities
- Identification and authentication failures
- Software and Data integrity Failures
- Insufficient logging and monitoring
- Server Side Request Forgery (SSRF)

# Internet

- Internet : vecteur physique considérable de vulnérabilité
  - Tous les réseaux sont connectés
  - De plus en plus d'objets sont connectés en réseaux et accessibles
  - Le commerce électronique est omniprésent
  - Augmentation de la bande passante
  - Les informations peuvent circuler très vite
  - Le Time to Market diminue, au détriment des tests et de la sécurité des applications
- **CERT**
  - Computer Emergency Response Team
  - Met à jour la liste des attaques et les contre-mesures à appliquer
- CVE ( Common Vulnerability and Exposure)
  - Toutes les failles sont théoriquement répertoriées par ce site
  - En inverse, possibilité de trouver des exploits (vuldb, exploit-db, etc…)

# La Triade

- Disponibilité (availability)
- Intégrité (integrity)
- Confidentialité (confidentiality)




- Preuve
- Non-répudiation

→ Contrôle des accès

# Contrôle des accès

- 3 catégories
  - Administratives (politique de sécurité)
    - Qui, où, comment, etc
  - Technique/logiciel
    - Parefeu, identification, password, etc…
  - Physique
    - Accès aux locaux, aux prises, etc..

➡ Nécessité de pouvoir vérifier le fonctionnement

- journalisation des actions
- Durée de conservation des logs

# Identification/Authentification

- 2 concepts différents
- Authentification
  - 4 facteurs possibles
    - utiliser une information que seul le commettant connaît (ce que l'on connaît)
    - utiliser une information unique que seul le commettant possède (ce que l'on possède)
    - utiliser une information qui caractérise le commettant dans un contexte donné (ce que l'on est)
    - utiliser une information que seul le commettant peut produire (ce que l'on sait faire).
  - simple (1 facteur), forte( >=2 facteurs)

    **MFA – MULTI FACTOR AUTHENTICATION**
  - SSO ( Single Sign-On) -> 1 seule authentification pour tout

# Authentification(1)

- Password
  - Sécurité faible
    - Souvent simple, stockage ou transmission en clair, etc
    - Augmentation de la difficulté en rajoutant des contraintes
    - Limiter le nombre d'essais
- Biométrique
  - Empreinte digitale ou rétinienne, voix, main, faciale, etc..
  - Problème faux positifs ou faux négatifs
- Carte à puce
  - Clé statique ou dynamique
- Ticket
  - Dédié pour kerberos

# Rappel : le réseau

- Modèle en couches
  - **Modèle OSI : 7 couches**
  - **Modèle TCP/IP : 4 couches** → création 1973
  - **Basé sur IP au niveau 3**
    - Mode non connecté, sans mécanisme de sécurité ( IPv6 n'est pas encore beaucoup utilisé)
  - **Basé sur TCP au niveau 4**
    - Fiable, assure la retransmission des paquets perdus et une gestion « simple » de la bande passante -> algorithme new Reno ou Cubic
  - **Basé sur UDP au niveau 4**
    - Non fiable, non sécurisé
  - **Niveau applicatif**
    - Protocole plus ou moins récent, sécurisé ou non

# Les différentes adresses

- Au niveau 2
  - Adresse MAC (adresse physique)
  - Théoriquement fixe, unique sur le réseau local
  - Quelques bibliothèques permettent de créer des trames directement à ce niveau (pcap, scapy)

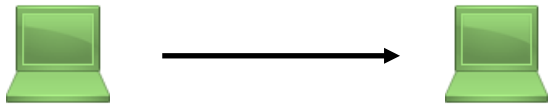
- Au niveau 3
  - Adresse IP ( adresse logique)
  - Adresse Privée/publique
  - Change au gré des utilisateurs

- Au niveau 4
  - Port ( réservé en-dessous de 1024)

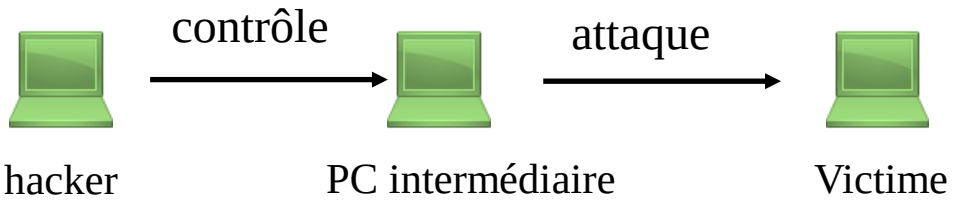
Si aucun port n'est ouvert, sécurité accrue, obligation de passer par le niveau 2 ( même site)

# Les différents types d'attaque

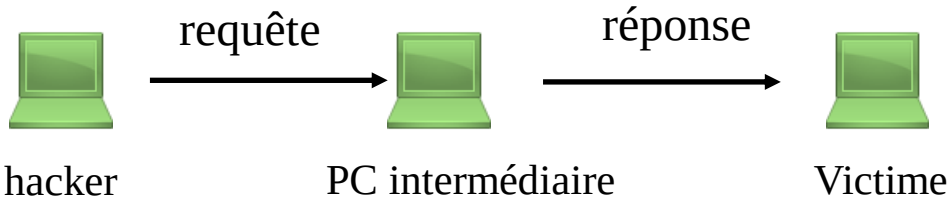
- Attaque directe



- Attaque indirecte par rebond




- Attaque indirecte par réponses



# Cartographie du réseau (1)

- Renseignement sur le réseau
  - Recherche d'informations publiques
    - DNS, whois, ….
    - Utilisation d'utilitaire (dig, host, ….)
    - Test des chemins via traceroute/tracert ( fonctionnement du TTL) , cheops-ng, ….
    - Envoie d'un mail avec mauvais correspondant
  - Balayage
    - Découvrir les machines présentes
    - Le protocole ICMP
    - ICMPv6 a encore plus de fonctionnalités…
    - Présence de filtrage ( utilisation du TTL, et ICMP)
      - Logiciel firewall, nmap

# Cartographie du réseau (2)

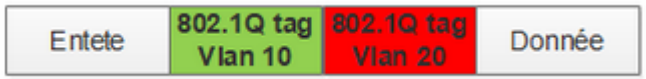
- Renseignement sur le réseau
  - Balayage sur les ports
    - Quels ports sont ouverts ?
    - Envoie d'un paquet, et attente du retour
    - Ex : envoie de syn sur un port,
      - Si retour = syn+ ack , port ouvert
      - Si retour= rst, port fermé
      - Si pas de retour, possibilité pare-feu.
  - Logiciel nmap, netdiscover, netcat, ….
    - Scan Half open syn, Null, xmas,…. (option de nmap)

Méthodes assez détectable…. Sauf si étalé dans le temps.

# Attaque sur switch

- Augmentation de la sécurité : VLAN
  - Protocole 802.1Q permet de simplifier la gestion/trunking

- Saut de VLAN
  - Switch spoofing
    - (utilisation du protocole Dynamic Trunk Protocol)
    - Objectif : sa faire passer pour un switch, puis configurer liaison trunk avec le switch cible
  - Double encapsulation
    - Le vlan 10 est enlevé par le 1er switch
      - Permet d'atteindre via le second switch le vlan 20



# Attaque sur une machine

- Plusieurs étapes
  - Recherche des ports ( services ) ouverts
  - Recherche des applicatifs et leur version qui tournent
  - Recherche via les BDs d'exploit si faille présente
  - Une fois, prise en main
    - Mise en place d'une backdoor
    - Utilisation d'un centre Command & Control (C&C)
- Protection
  - Limiter le nombre de ports ouverts
  - Mettre à jour les logiciels
  - etc…

# Attaque sur un réseau (1)

- ARP spoofing
  - Envoies-en continue de trames ARP
  - Facilement détectable sur des switches manageables
- IP spoofing
  - Existe, mais très difficile à mettre en place
  - Utiliser pour le DOS
- Man in the middle
  - Faire transiter les données via la machine pirate
    - Soit 2 communications distinctes
    - Soit comme routeur ( mais impossible d'intercepter conversation chiffrée)

# Attaque sur un réseau (2)

- DOS ou DDOS
  - objectif : saturation des connexions réseaux d'un PC
    - Ping flooding
    - Attaque smurf ( idem, mais icmp en broadcast)
    - Attaque TCP syn
    - Epuisement des connexions TCP
  - Contre-mesure
    - test de la taille des paquets
    - test des adresses source et destination (ainsi que loop-back, unicast, multicast...)
    - test de la fragmentation
    - test du nombre de SYN (contre-attaques TCP)
    - Load-balancing

# Attaque sur un réseau (3)

- Installation de virus
  - Phishing
  - Via sites webs infectés
  - Via des exécutables, des documents, etc….
  - Faille logicielle
- Prise en main via un BotNet
  - Utilisation : DDOS, spam, minage, bruteforcing, …
  - Raison économique ( location de botnet )

# Attaque sur le DNS

- DNS est encore un protocole en clair
  - Protégé contre DDOS ( suite à l'attaque de 2007)
    - Utilisation des adresses anycast
  - Attaque possible sur les caches DNS
    - Empoisonnement du DNS
    - Faire correspondre une fausse @IP à un nom

  Utilisation de DNSSec

# MITM

- Attaque Man in the Middle
  - Plusieurs vecteurs d’attaque possible
  - Objectif : attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre puisse se douter que le canal de transmission entre elles a été compromis.

# Sécurisation d'un réseau

## Défense en profondeur

Objectif : Ralentir l'attaquant

Aucun système n'est sûr

-> faille 0-day

-> nouveau virus

-> indiscrétion d'une personne,….

-> bug dans un logiciel

- revue de code
- test de conformité, de fuzzing, ….

# Sécuriser un réseau

- Equipement possible
  - Switch
  - Routeur ???
  - Pare-feu
  - IDS/IPS (TAP : Terminal Access Point)
  - WAF  (Web Application Firewall)
  - RASP (Runtime Application Self-Protection)
  - proxy , reverse proxy
  - Serveur VPN, serveur cryptographique

# Sécuriser un réseau (2)

- Moyen logiciel
  - Durcissement du noyau des serveurs
  - Utilisation d'adresse privée
  - NAT
  - Chiffrement des données
  - VLAN
  - Interdire certains protocoles ou fonctionnalités (DTP, netbios, ttl de icmp, ….)
  - Antivirus, EDR (Endpoint Detection and Response)
  - Sauvegarde des données