Serveur de jeux : dimensionnement, gestion, optimisation et sécurité

CM2 : Sécurité et monitoring

Mickaël Martin Nevot

V1.10.0

Sécurité informatique

- **Intégrité des données** : pas d'altération non voulue
- **Confidentialité** : mise en place d'habilitations
- **Disponibilité** : accès permanent
- **Non-répudiation** : transaction correcte
- **Authentification** : accès limité
- Niveau :
  - Utilisateur
  - Technologie
  - Données
  - Physique (matériel, infrastructure)

Généralités

- L'information est partout :
  - De plus en **plus de données**
  - Des données de plus en **plus importantes**
- Connaître le système d'information pour le protéger
- Savoir identifier la menace
- Instaurer de bonnes pratiques de sécurité :
  - Sécurité d'un système = sécurité du maillon le plus faible
- **Auditer** son système
- Apprendre à se défendre : ***ethical hacking***

Famille de Hackers

- ***Script kiddies*** (pirates néophytes)
- ***Black hats*** (hors la loi)
- ***White hats*** (but « honorable »)
- ***Gray hats*** (mélange de *black hats* et de *white hats*)
- ***Hackers* universitaire** (militants *open source*)
- *Hackers* ? *Streakers*, *Jumpers*, etc.

Méthodologie d'une attaque

- Collecter des informations (**prise d'empreinte**) :
  - Google, Facebook, etc.
  - Les êtres humains sont bavards
  - Internet non-anonyme : *surfer*, « *bloguer* », etc.
  - Interroger les services lancés

    Apache (serveur Web), FTP, SNMP pour contrôle partiel du réseau
  - **Pile TCP/IP** sur un serveur

    Permet de connaitre : Système d'exploitation, IP active, ports ouverts, etc.
- Repérer les **failles** :
  - Connaitre les failles connues
  - Ne pas tenir compte des non fondées

Méthodologie d'une attaque

- **Intrusion** dans le système (appelé ***exploit***) :
  - Ne pas laisser de traces (**journaux système**)
  - Extension des privilèges
  - Collecte d'informations
- **Assurer son accès** :
  - « Écouter » le trafic
  - Etendre son accès à d'autres machines du réseau
  - Faciliter son retour (***backdoor, rootkit***)
  - Effacer ses traces
- **Exploitation**

Ingénierie sociale

- Cible du « piratage » : l'**être humain** (tous concernés)
- Attaquant : charismatique, manipulateur, imposteur
- Moyens utilisés :
  - Téléphone, fax, *e-mail*, courrier, *tailgating*, etc.
- Contre-mesures :
  - **Matrice de sensibilité** : régit l'accès aux informations
  - Détecter les attaques : se demander pourquoi ?
  - **Sensibilisation** générale
    (y compris standardistes, stagiaires, etc.)

Leviers de l'ingénierie sociale

- Leviers psychologiques :
  - **Absence de méfiance** : pas forcément besoin de dialogue
  - **Crédulité** : utilisation d'un faux prétexte (argent ou gain facile)
  - **Ignorance** : non-sensibilisation à la sécurité des collaborateurs
  - **Confiance** : favoriser le réflexe d'échange (fausse identité, etc.)
  - **Altruisme** : susciter l'envie d'aider
  - **Besoin d'aide** : faire croire que la cible a besoin de notre aide
  - **Intimidation** : créer une situation de peur ou de doute
- Autres leviers :
  - ***Hijacking*** : détournement physique d'une personne

Souvent appelé *old-school hijacking* (méthode à l'ancienne !)

Ingénierie sociale : bonus

- https://youtu.be/lVIxPWTv_fo

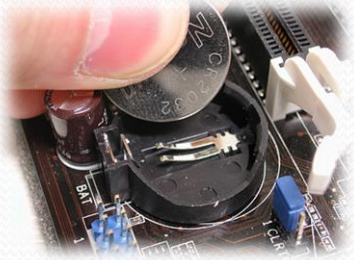
Différence chiffrement/codage

- **Chiffrement** (ou cryptage) : protège l'information
  - Exemples : AES, Blowfish, RSA
- **Codage** (ou hachage) : transformation des données
  - Exemples : MD5, SHA, LM
- Mot de passe :
  - Données encodées : MD5, LM, etc.
  - Piratage :
    - ***Brute force***
    - Avec **table *Rainbow***


```
00000000h: 6F AF B2 DD 24 00 00 00 32 24 00 00 00 00 00 00   o¯²Ý$...2$......
00000010h: 75 96 48 46 5E 00 00 00 F4 45 00 00 00 00 00 00   u-HF^...ôE......
00000020h: 89 A5 A4 31 66 00 00 00 97 A4 00 00 00 00 00 00   ‰¥¤1f...—¤......
00000030h: 5E C8 02 7F 1C 00 00 00 A7 C4 00 00 00 00 00 00   ^È.□....§Ä......
00000040h: 74 B6 B4 1A 2D 00 00 00 A7 C4 00 00 00 00 00 00   t¶´.-...§Ä......
00000050h: 37 08 CE 19 57 00 00 00 11 0C 01 00 00 00 00 00   7.Î.W...........
00000060h: 82 C0 1C 3A 5E 00 00 00 0F 36 01 00 00 00 00 00   ‚À.:^....6......
00000070h: F2 41 2F BD 94 00 00 00 5D 60 01 00 00 00 00 00   òA/½"...]`......
00000080h: 47 C5 6D 61 65 00 00 00 5D 60 01 00 00 00 00 00   GÅmae...]`......
```

Failles physiques (matériel éteint)

- Bios protégé (par mot de passe) :
  - Vider le **CMOS** (cavalier ou pile)



  - Déchiffrer le mot de passe (matériel avec mémoire ***eeprom***)
- Pas de mot de passe bios :
  - Démarrage sur ***livecd*** / **clef USB**
  - Windows : ***dumper*** la **base SAM**, déchiffrer mot de passe
  - Linux : piratage du **boot**, etc.

Failles physiques (matériel allumé)

- Relever les mots de passe de session Internet
- Révéler les astérisques d'un champ mot de passe
- Récolte d'informations utilisateur (automatisée)
- **Clef USB U3** piégées (auto exécutables)
- ***Dump* mémoire** (vive) :
  - Mémoire vive effacée **après** qu'elle ne soit plus sous tension
  - **Temps de rémanence** augmentable (refroidir la mémoire)
  - On peut dumper la mémoire durant ce temps
- ***Keyloggers*** (physique ou logiciel)
- **Flux ADS** : exécutable caché dans un fichier

Mouselogger

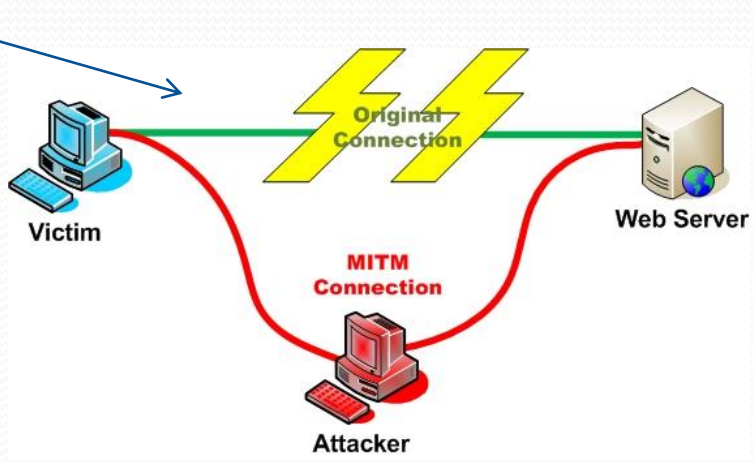
Nouveau : un *Keyloggers* physique version souris !

Failles réseaux

- **Tunnel SSH** : connexion sécurisée sur un serveur **Proxy**
- **DoS/DDoS** : déni de service par attaque « ***syn flood*** »

  Un DoS est simple à contrer (blocage d'adresse IP dans le pare-feu)
  Un DDoS est une attaque de déni de service **distribuée** (difficile à contrer)

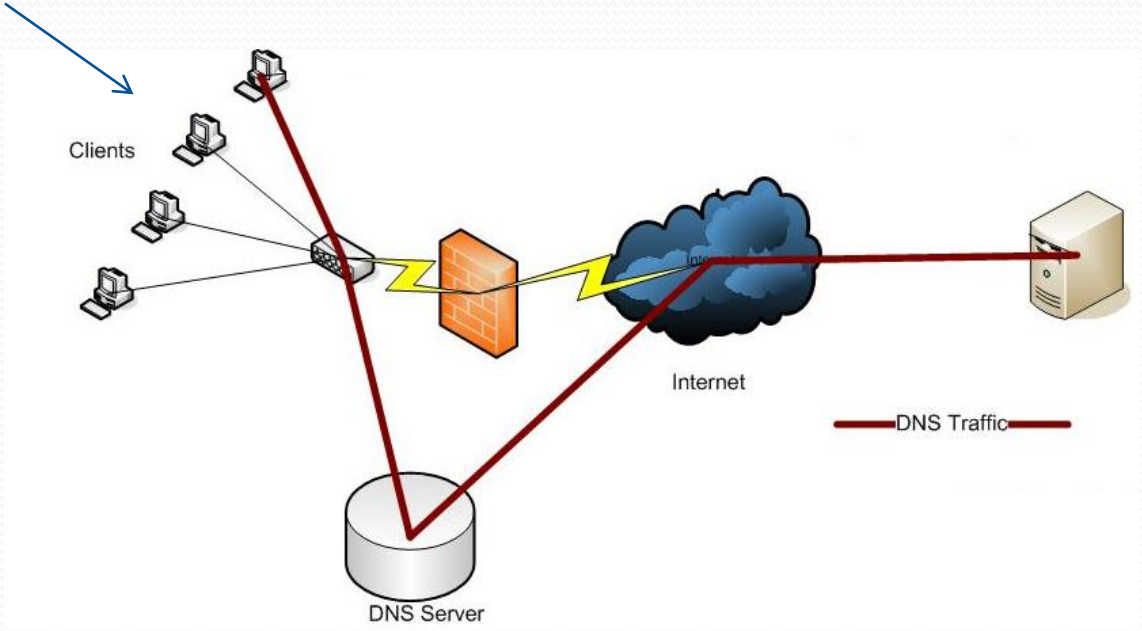
- ***Sniffing*** : espionne les données transférées par un réseau
- ***Man in the middle*** (MITM) : imposture adresse IP/MAC



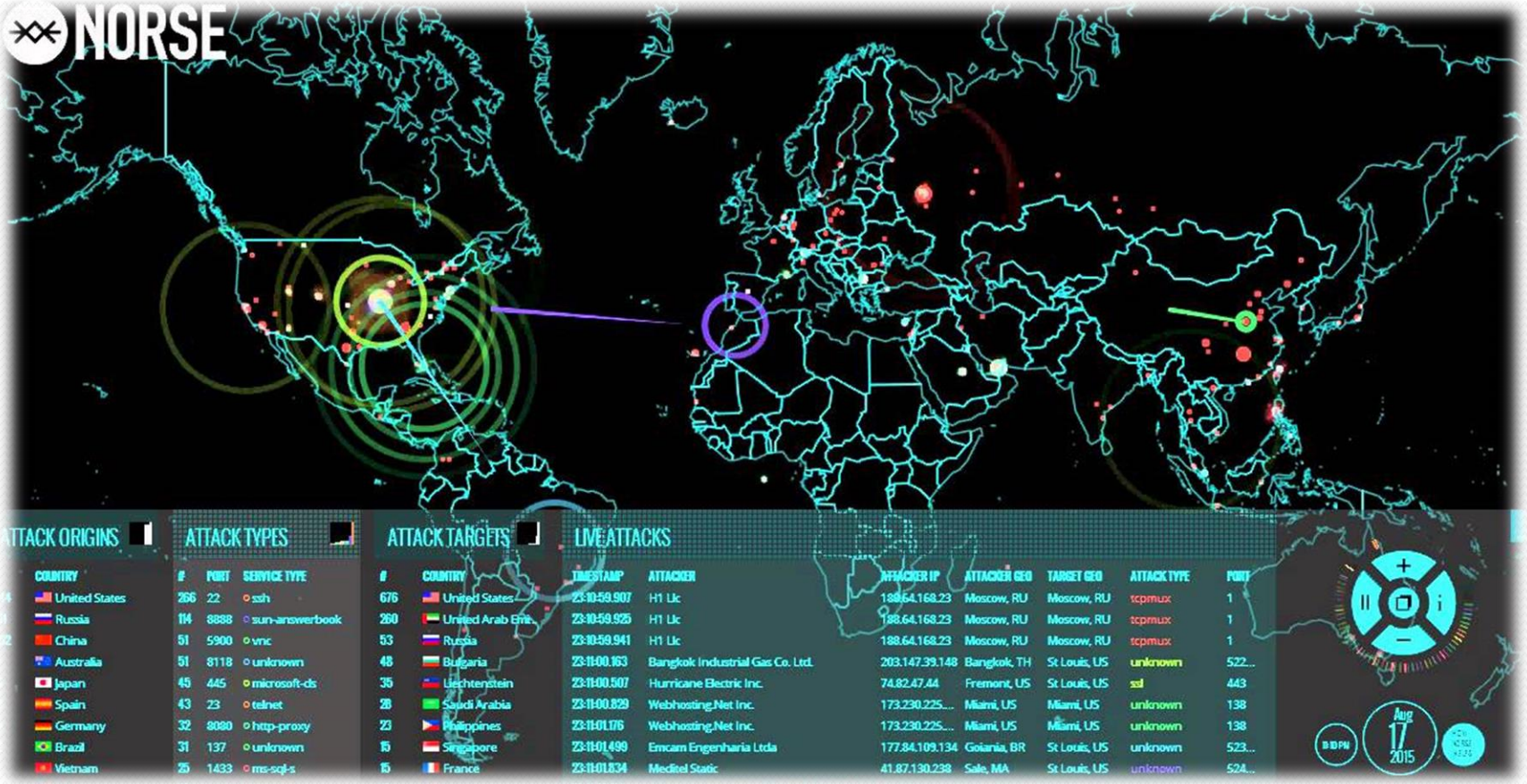
Failles réseaux

- Failles **Wi-Fi** :
  - « Cracker » un réseau **WEP**
  - « Cracker » un réseau **WPA**

  Se connecter sans en avoir le droit
  - ***IP over DNS*** : pirater un *hotspot* Wi-Fi



Attaques DDOS en direct



- http://map.norsecorp.com/#/

Failles Web : analyse de site

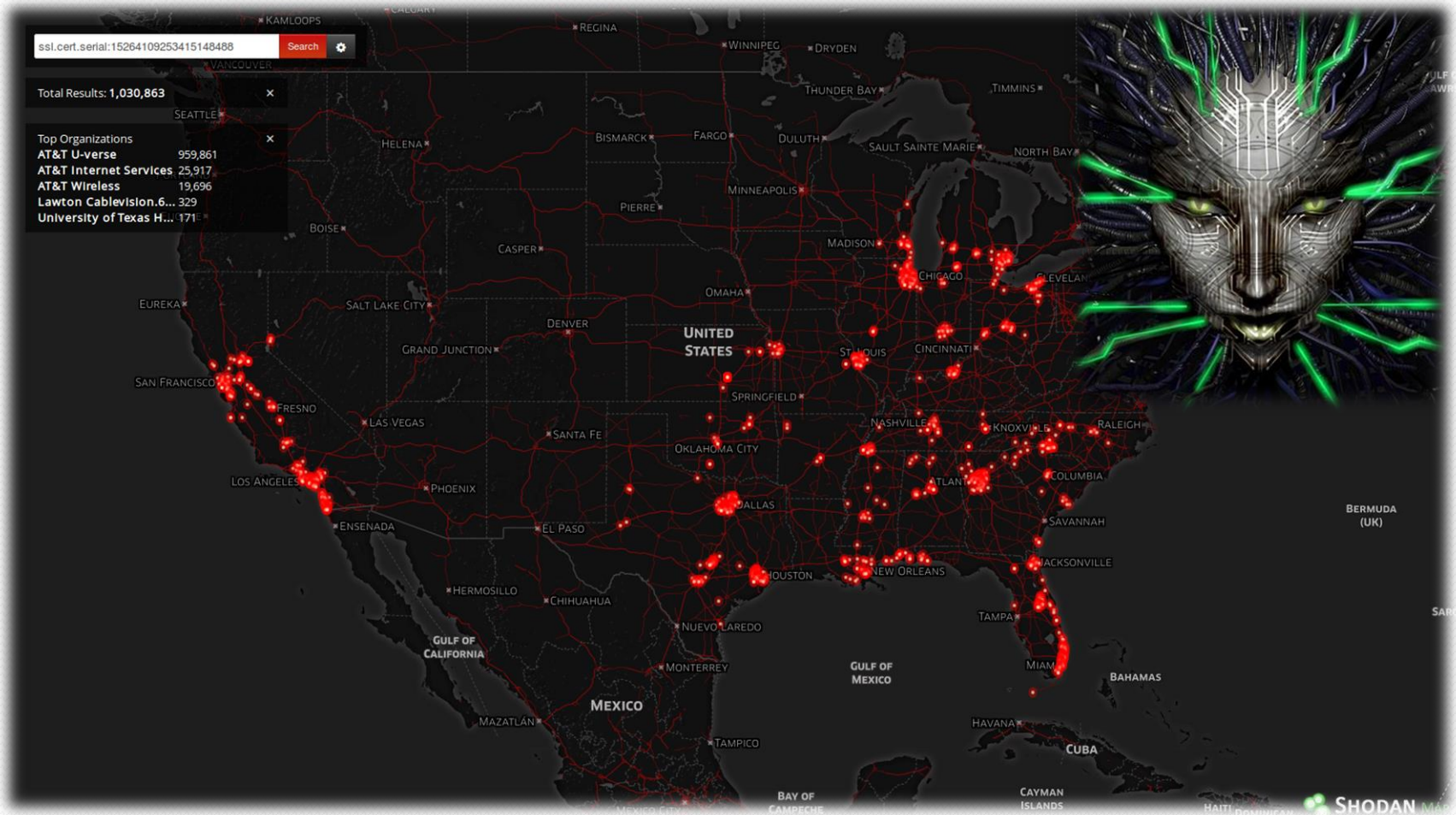
- Partie visible :
  - **Statique** ou **dynamique** ? (y a-t-il une **URL *rewriting*** ?)
  - Les variables utilisées ? (méthode **GET** ou **POST**)
  - Les champs des formulaires ? Des **champs cachés** ?
  - Existence de ***cookies*** ?
  - Répertoires d'images, vidéos, etc. ?
  - Existence de **JavaScript** ?
  - Existence de **répertoires accessibles** ?
- Partie cachée :
  - Intercepter les échanges entre navigateur et serveur Web
  - Envoi massif de requêtes avec un ***fuzzer***

Failles Web : attaques

- Modification de chemins et URL :
  - Changement d'inclusion de fichier
  - **Injection de code JavaScript**
- **Injection SQL** (par l'intermédiaire des formulaires)
- Modification des **entêtes** (pirater une authentification)
- Modification des ***cookies***
- **Dépôt de fichiers** malicieux

Exemple : un virus à la place d'une image devant servir d'avatar sur un forum

Shodan : ports non protégés

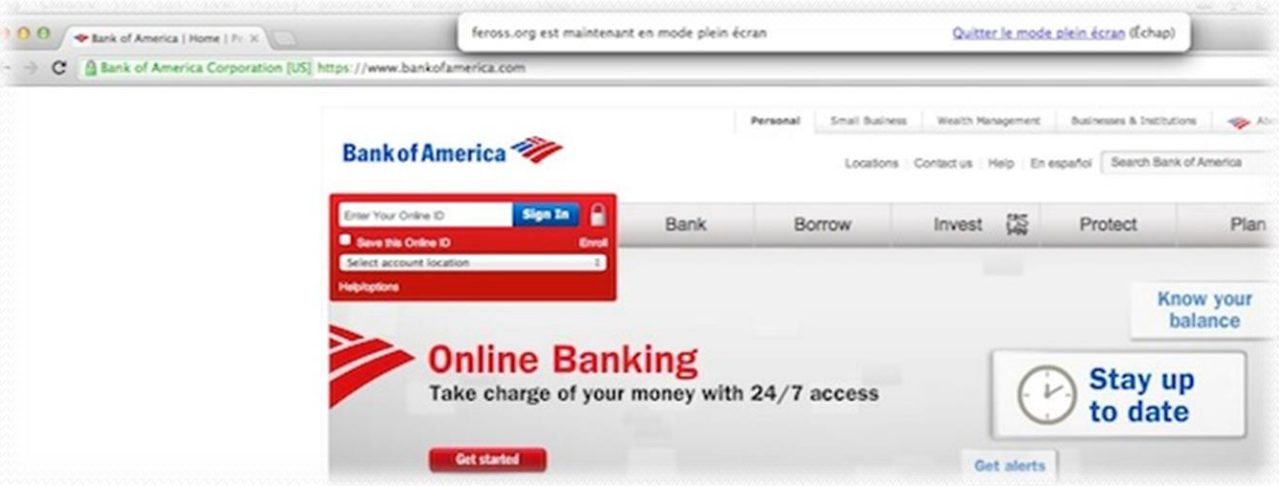


- https://www.shodan.io/

Injection SQL insolite

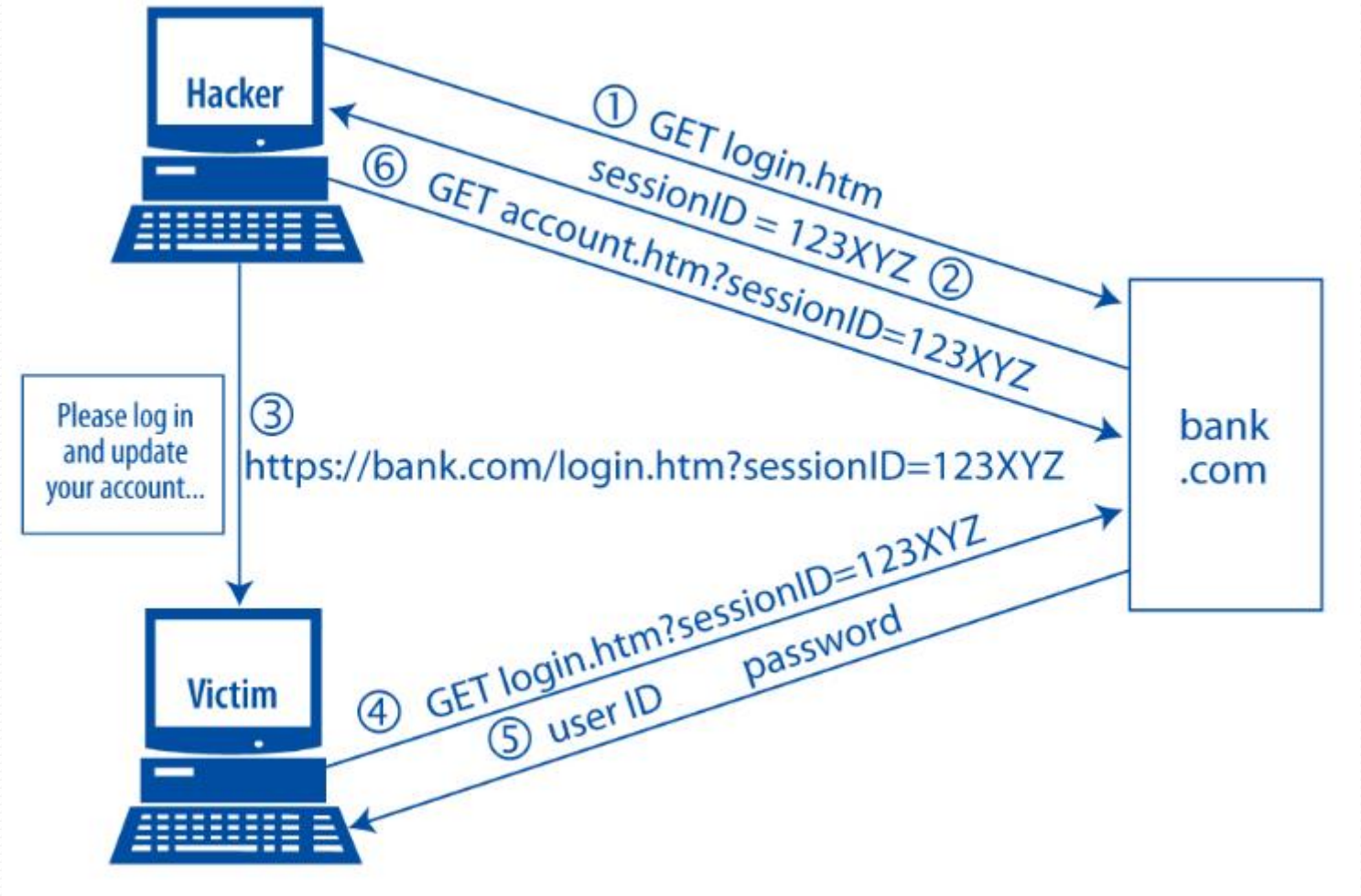
Hameçonnage (Fishing)

- **Faux site Web** (usurpation d'identité)
- Utilisation *d'e-mails* et ***cross-site scripting*** **(XSS)**
- Cécité au changement :
  - Représentation lacunaire faite d'observations partielles



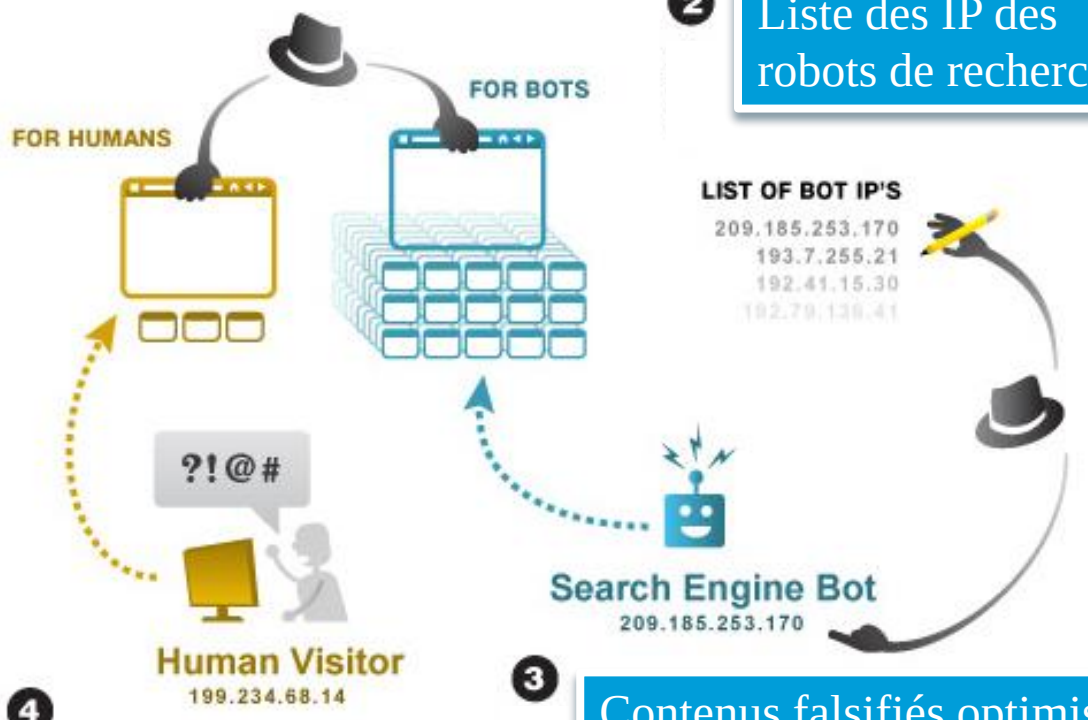
- http://feross.org/html5-fullscreen-api-attack/

Failles Web : hijack de session



Failles Web : Cloaking

1. Contenu différent pour un internaute ou un robot (IP)



2. Liste des IP des robots de recherche

3. Contenus falsifiés optimisés pour le référencement

4. Contenu en décalage avec le référencement

Failles applicatives

- **Élévation de privilèges** (`suid`, `sgid`) : exécuter avec privilèges du **propriétaire** du fichier sans besoin d'authentification de ce dernier
- ***Shellcodes*** : code binaire (ou hexadécimal) exécutable capable de lancer une invitation de commande
- ***Buffer overflows*** : exploitation d'un bogue pour détourner un programme afin de lui faire exécuter des instructions qu'il a introduit dans le processus

Difficile à mettre en place mais très difficile (parfois presque impossible) à contrer !

Virus, spywares, chevaux de Troie

- **Virus** : logiciel malveillant se reproduisant grâce à un programme hôte :
  - Classique
  - Virus de *boot*
  - Macrovirus (macro Microsoft Excel, etc.)
- **Ver** : se reproduit juste grâce au système, se propagent par le réseau, a des actions discrètes et non-destructrices
- ***Spyware*** : logiciel espion (collecte les données et les envoie à un tiers : hacker ou entreprise)
- **Cheval de Troie** :
  - Création de *backdoor* (« porte de derrière »), ne se reproduit pas

Mots de passe

- Mot de passe **complexe** (*bios*, session, etc.) :
  - Long (plus de six caractères)
  - Caractères alphanumériques plus caractères spéciaux
  - Pas de mot existant, date de naissance, nom du conjoint, etc.

Bonnes pratiques

- Changer souvent de mot de passe
- Interdire les *boots* autres que disque dur
- **Verrouiller sa session** utilisateur en cas d'absence
- Utilisation d'**antivirus** et d'**anti-*spyware***
- Filtrer vos données (pour éviter les injections)
- Système d'authentification robuste (pas juste un *cookie*)
- Configuration muette du serveur Web

Bonnes pratiques

- *Monitoring* des **processus**
- *Monitoring* des **journaux systèmes**
- **Mise à jour** (automatique ?) des logiciels
- Faire des sauvegardes des données
- Virtualisation :
  - ***chrooting*** (racine virtuelle dans un répertoire)
  - **Noyau en espace utilisateur** (plusieurs noyaux virtuels)
  - **Machine virtuelle** (émulation d'une machine complète)
  - **Paravirtualisation** :
    - Machine virtuelle plus noyau en espace utilisateur

Quelques outils

- `whois`, `traceroute` , `host` : connaitre l'architecture réseau
- `Nmap`, `Siphon` : scanner les ports TCP
- `Snmpwalk` : interroger le service SNMP
- `Nessus`, `SecurytyFocus` (site Web) : listes les vulnérabilités
- `Netstat` : connaitre services et ports ouverts
- `Netcat`, `cryptcat` : créer une *backdoor*
- `cloak2` : effacer ses traces dans les journaux systèmes
- `domainename` : rechercher une machine sur un réseau
- `backtrack` : *live distribution* d'audit de systèmes
- `John the Ripper` : déchiffrer des mots de passe

Quelques outils

- `Ophcrack` : utiliser des tables *rainbow*
- `Cain&Abel` : boîte à outils audit de sécurité
- `IE Pass view`, `IE History View` : données navigateur
- `X-Pass` : révéler astérisques d'un champ mot de passe
- `Switch blade` : récupérer données utilisateur
- `msramdmp` : *dumper* la mémoire (vive)
- `SpyAgent` : *keylogger* logiciel
- `ssh` : se connecter en sécurité, faire un tunnel SSH
- `hping2` : effectuer des attaques *syn flood*
- `wireshark` : *sniffer*

Quelques outils

- `ettercap` : effectuer des attaques *man in the middle*
- `arpwatch` : contre-mesure *man in the middle*
- `aircrack` : boîte à outil pour craquer les réseaux Wi-Fi
- `iodine` : effectuer de l'*IP over DNS*
- `Web Developer` : extension Firefox pour l'analyse Web
- `SQL Inject Me` : extension Firefox pour l'injection SQL
- `Burp Suite`, `WebScarab` : intercepter les échanges Web
- `wfuzz` : *fuzzer* Web
- `hijackthis` : programme de défense très utile

Quelques outils

- `useradd`, `usermod`, `userdel` : gérer utilisateurs
- `groupadd`, `groupmod`, `groupdel` : *idem* groupe
- `chown`, `chgrp`, `chmod` : gérer permissions
- `ps`, `top` : voir les processus d'un système
- `SeLinux`, `AppArmor` : gérer les privilèges
- `Promox VE` : effectuer de la paravirtualisation
- `JMeter` : tester la performance de serveurs

Conclusion

- Ce cours couvre **au plus 90 – 95 %** des piratages actuels Le reste est :
  - Très difficilement sécurisable
  - Des ***exploits*** inconnus ***(zeroday)*** :
  - Bonus : https://youtu.be/lVIxPWIv_fo

    les Hackers ont **toujours** une longueur d'avance !

- Comment agir contre ces cas là ?
  - Faire appels à des tiers (garanties/assurances) pour les données très sensibles (informations de cartes bleues, etc.)
  - Ne pas s'attirer les foudres (**éthique correcte)**
  - Faire preuve d'**humilité** (avoir une solution en cas de perte totale d'un serveur ou d'un réseau)

Liens

- Documents classiques :
  - Livres :
    - ACISSI. *Sécurité informatique – Ethical Hacking*.
    - Frank Owens, L@tz@rus. *Hacker's Blackbook*.
  - Documents :
    - Adam Ouorou. *Optimisation robuste pour le dimensionnement des réseaux de télécommunications*.

Crédits

Auteur

Mickaël Martin Nevot
mmartin.nevot@gmail.com

Carte de visite électronique

Relecteurs

- Christophe Delagarde
- Marion Livoy

Cours en ligne sur : www.mickael-martin-nevot.com