Le piratage:

À la portée de tout le monde ?

Agenda de la présentation

- Les attaquants et leurs motivations
- Les différentes provenances et sortes d'attaques
- Les étapes d'une attaque
- Les outils
- Parce qu'un "hack" vaut 1000 mots… Des démos !!!

Qui sont les attaquants

- Script Kiddies
- Pirates professionnels / Mercenaires (espions/compétiteurs)
- Terroristes / Crime organisé
- Employés (volontairement et à leur insu) – Parfois les plus dangeureux

Motivations

- Argent (espionage, avantage concurentiel, mercenaire, etc…)
- Notoriété, gloire, réputation, etc…
- Politique / Activisme
- Parce que je peux… (opportunisme, apprentissage/découverte)
- Terrorisme (attaques et financement)
- Applications militaires

D’où proviennent les attaques

- Server-side Attacks (de l’externe)
- Client-side Attacks (de l’interne)
- Social Engineering (les gens)
- Wifi (interne et externe)
- Médias amovibles (Jeton USB et autres)

Étapes d'une attaque

- Reconnaissance (ramasser de l'info)
- Scanning (découvrir les failles)
- Attaque (exploiter les failles et vulnérabilités)

- Garder un accès (backdoor, porte dérobée)
- Effacer les traces (effacer/modifier les logs)

Reconnaissance

- Site Web:
  - Mission
  - Postes disponibles
  - Communiqués de presse
  - Adresses courriels
  - Et beaucoup plus…

- Adresses IP et autres informations
  - American Registry for Internet Numbers (ARIN)
  - Whois (Qui)
  - Nslookup (Quoi)
  - www.centralops.net ,Sam Spade

Reconnaissance (2)

- Google:
  - Requêtes (intitile, inurl, type, link, etc...)
  - Google Hacking DataBase (GHDB) – Johnny Long
  - Google Maps (endroits intéressants dans les environs)
  - Google Street View
  - Google Picassa
  - Google Cache
  - Google Groups
  - Google Blog

Reconnaissance (3)

- Réseau sociaux (Facebook, Twitter, LinkedIn)
  - (CeWL) -> Liste de mots (uname/passwd)
- www.123people.ca
- www.archives.org (Wayback machine)
- Outils (local)
  - Sam Spade
  - Foca (Metadata)
  - Maltego

Scanning

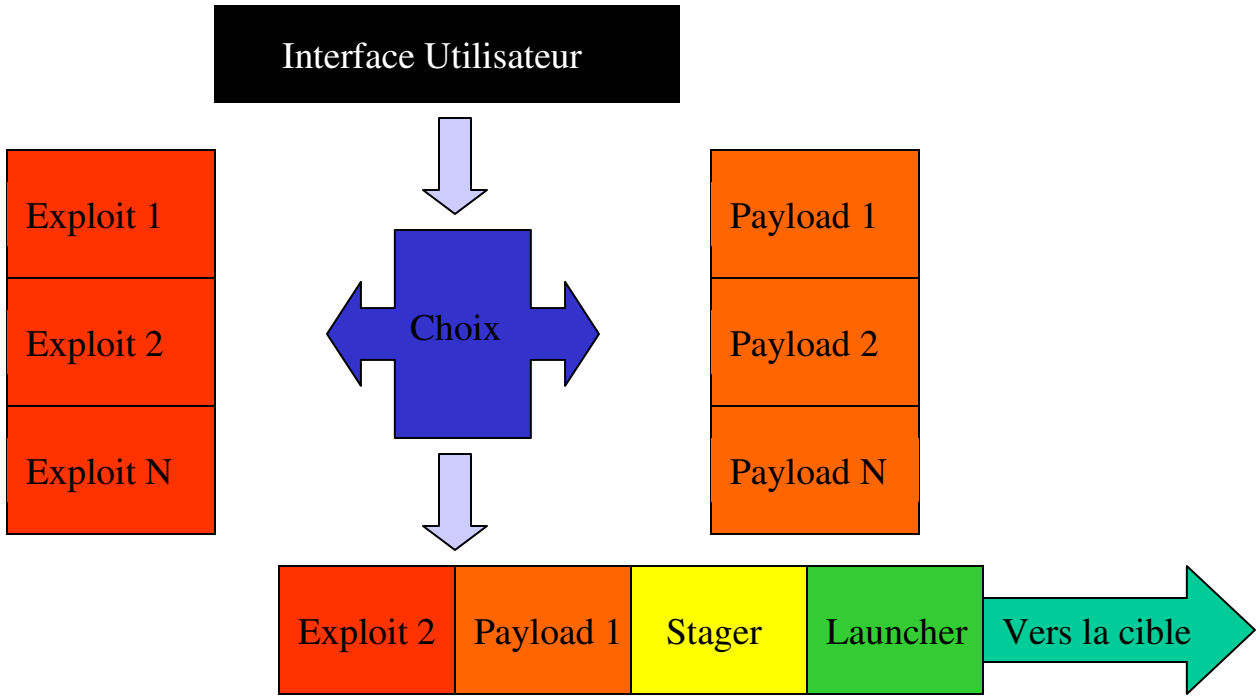
- Balayage de ports
  - Nmap
  - Découverte des ports ouverts (0 à 65535 - TCP & UDP)
  - Différents type de scans (connect, syn, etc…)

- « OS Fingerprinting » - Déterminer la version du OS
  - Actif: Nmap, Xprobe
  - Passif: p0f

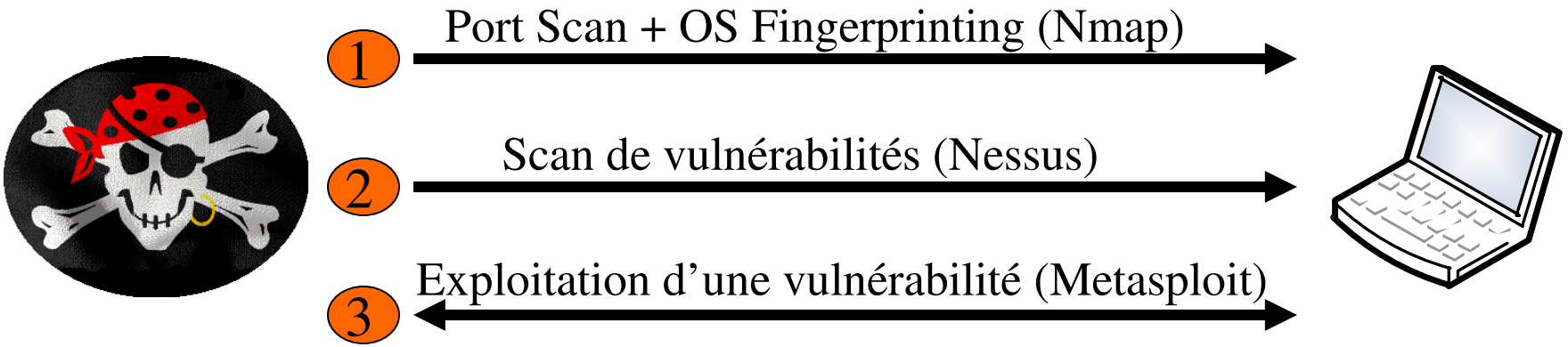
- Balayage de vulnérabilités
  - Nessus
  - Découverte des vulnérabilités dans le bût de les exploiter

Metasploit

Le “framework” **Metasploit** est un outil pour le développement et l'exécution d'exploits contre une machine distante.



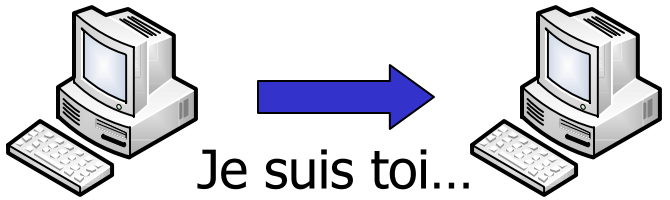
Attaque: Scénario#1 (Server-side)



“Shell is just the beginning”

- Cain
  - Sniffer un réseau commuté
  - Récupérer les mots de passe en clair & “hashes”
  - Cracker des mots de passes
  - Beaucoup d’autres possibilités

- Pass-the-Hash
  - GENHASH.EXE
  - IAM.EXE -> lsass.exe
  - WHOSTHERE.EXE



Attaque: Scénario#2 (Client-side)
(Info + Ingénierie sociale + courriel = !!!)

Vulnérabilités découvertes et documentés au cours des 3 dernières années:

~90

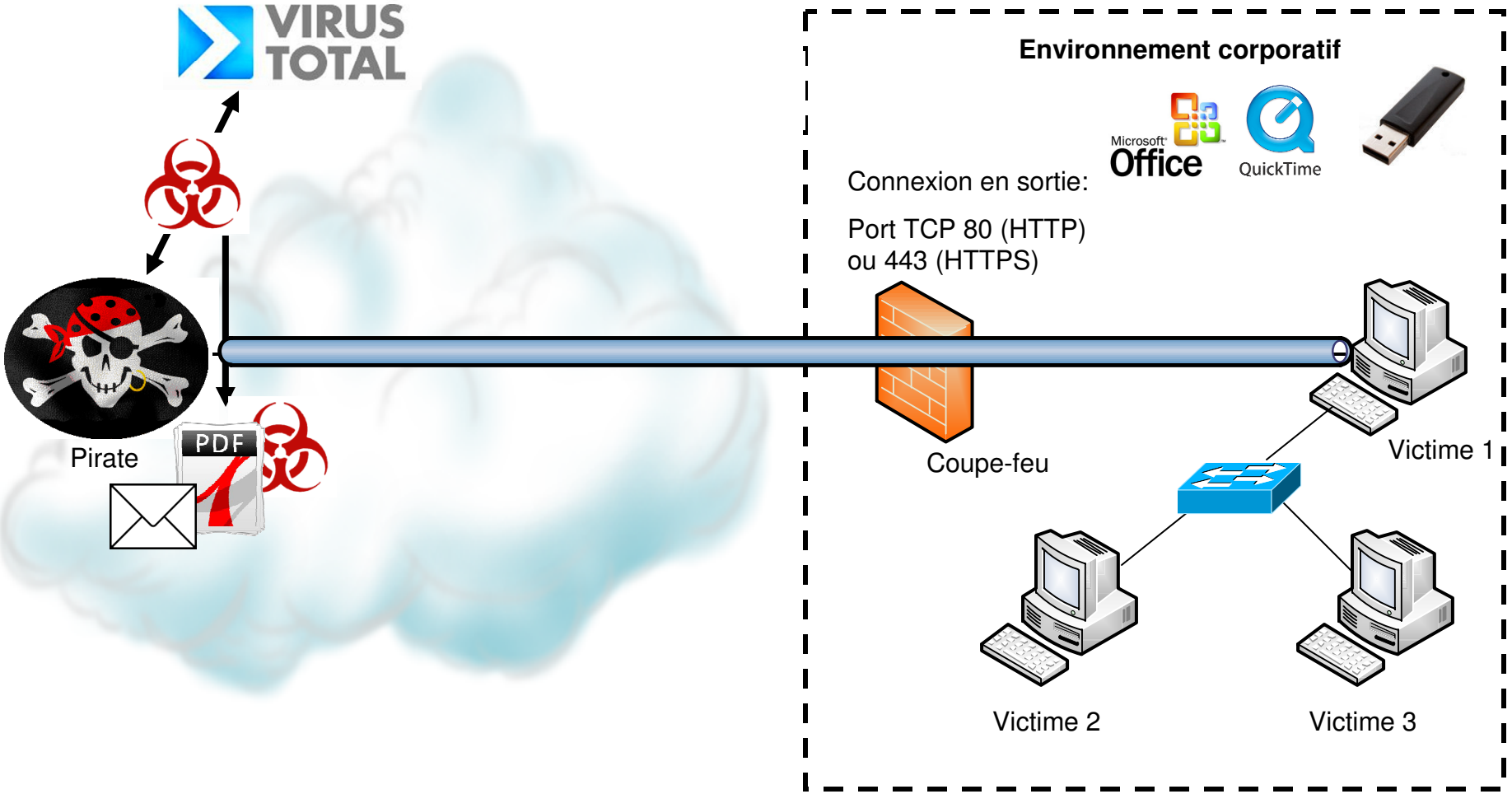
~200

~300

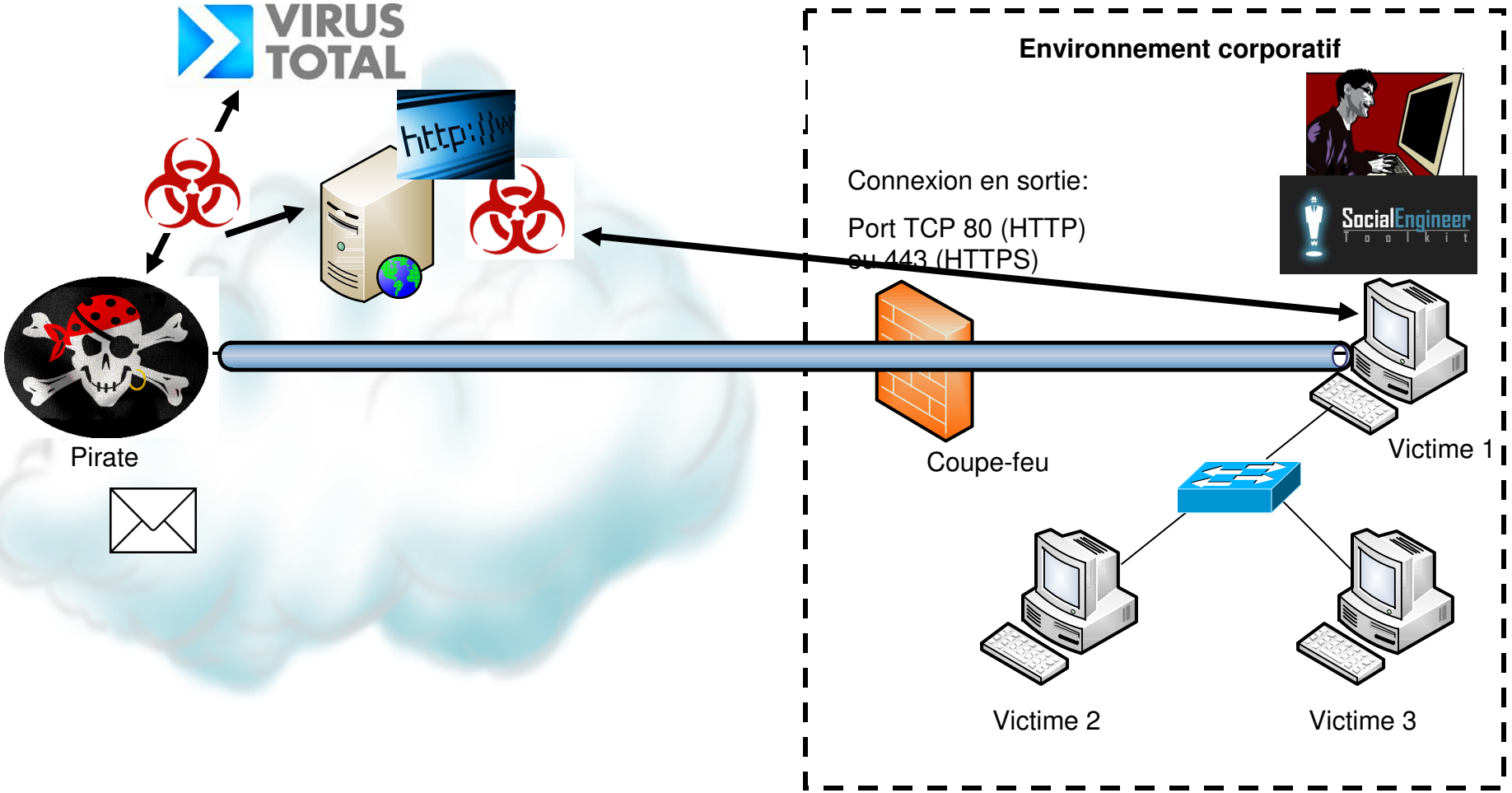
Est-ce que votre stratégie de mise à jour inclue ces produits? Vraiment…?

Sources: http://nvd.nist.gov/ et http://osvdb.org/

Attaque: Scénario#2 (Client-side)



Attaque: Scénario#3 (Client-side)



“Shell is just the beginning”

- Social Engineer toolkit (SET)
  - Clonage d’un site Web (redirection)
  - Interaction avec Metasploit
- Metasploit
  - Creation et encodage d’un “payload” malicieux (Meterpreter)
  - Serveur écoutant les requêtes entrantes des victimes
- Meterpreter (backdoor résident en mémoire injecté dans un dll)
  - Donne un plein accès au poste à la victime
  - Lister contenue du poste, les ps, Hashdump, pivot, etc…

Attaque: Scénario#4 (Jeton USB)

- Social Engineer toolkit (SET)
  - Jeton USB
  - Autorun.inf
  - "Payload" au choix de l'attaquant
  - Pourquoi pas un Backdoor?

- Sur le poste de la victime
  - Execution du backdoor avec les priv de l'utilisateur (admin?)
  - Connexion de la victime vers le pirate

Le Wifi

- Simple à sniffer (Netstumbler, Wireshark, Kismet, etc…)
- Filtrer par adresses MAC et cacher le SSID = Inutile !
- WEP, WPA, WPA2 -> Tous “crackables”
  - Faiblesse au niveau des initialization vector (IV)
  - Une authentification robuste est nécessaire
    - PEAP (Protected Extensible Authentication Protocol)
- Lorsque bien implanté, un réseau wifi peut-être aussi sécuritaire ou même plus qu’un réseau filaire.

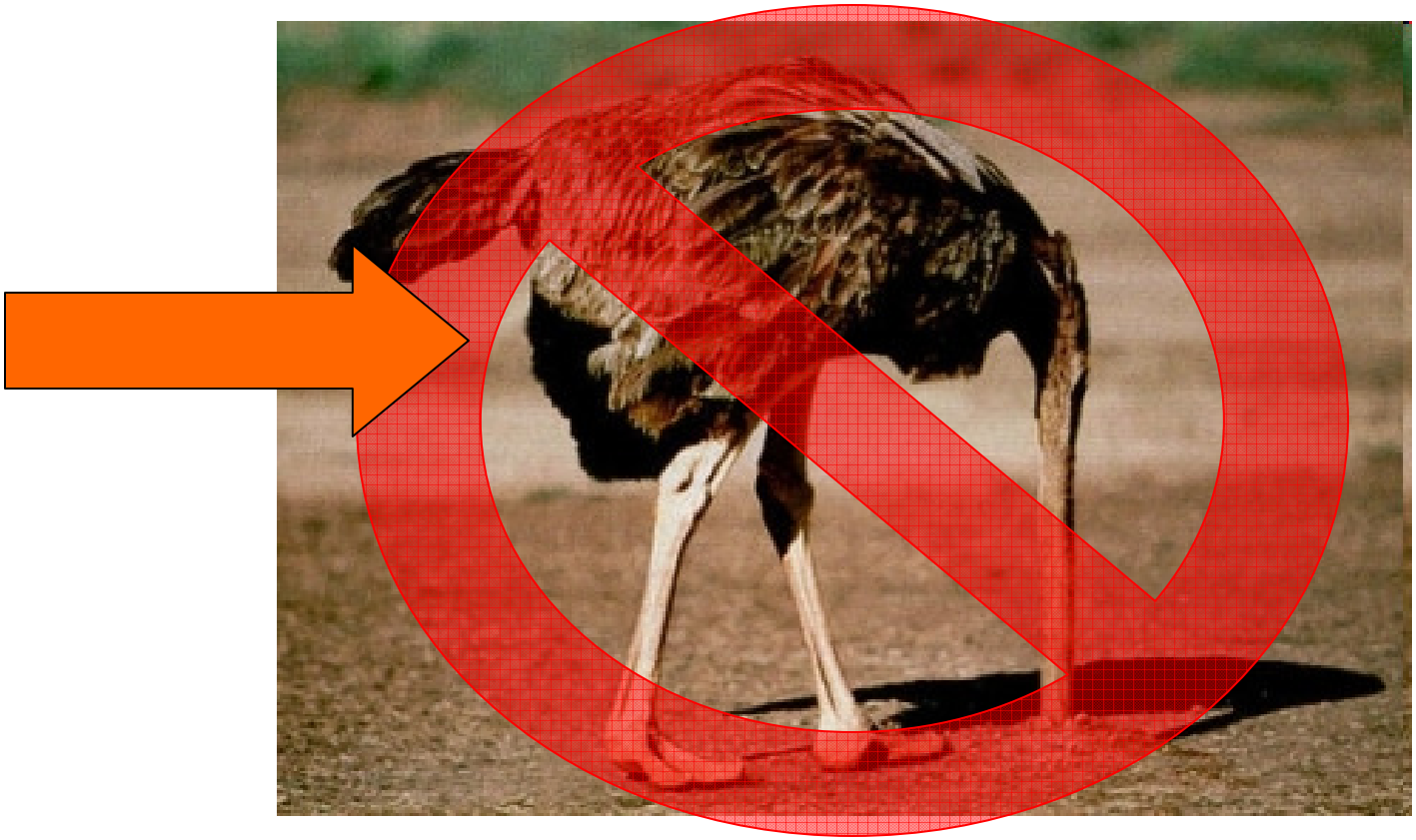
Le Wifi

- Aircrack-ng
  - Crack: WEP, WPA, WPA2 -> Preshared Key (PSK)
- Airpwn (Sniff le trafic wifi)
  - Inject du “faux” trafic (HTTP) - “Race condition”
- AirJack (MITM)
  - Désauthentifie, sniff, devient un AP, MITM
- Karma (Devient tout ce que vous demandez)
  - DHCP, DNS, HTTP, FTP, POP3, SMB
- Firesheep (Hijack des comptes Facebook, Twitter, etc…)
  - Add-on dans Firefox

Applications Web

- Command Injection
- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (XSRF)

Conclusion



Formation - SANS

- SANS Security 564 - Hacker Detection for System Administrator
  "Détection de pirates informatiques pour administrateurs de systèmes"
- SANS Security 504 - Hacker Techniques, Exploits & Incident Handling
- SANS Security 560 - Network Penetration and Ethical Hacking
- Info: http://cusin.ca ou michel@cusin.ca
- Services Professionnels Bell / Sécurité