

# Techniques et outils de piratage

## 1-Reconnaissance : Footprinting

Comprendre les attaques pour mieux se défendre

Mohamed Mejri

Mohamed.Mejri@ift.ulaval.ca

13 septembre 2016

# Plan

## 1 Introduction

## 2 Étapes du footprinting

- Information publique
- WHOIS
- DNS
- Réseau

## 3 Outils importants pour le footprinting

- Récapitulatif

# L'art de la guerre

## Connaitre votre ennemi

*"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."*

Sun Tzu, Art of War



# L'art de la guerre

**Ingédients d'une attaque** Pour qu'il y ait une attaque, il faut réunir les ingrédients suivants :

- Menace : agent de l'attaque ou celui qui fait l'attaque (p. ex., feux, pirate, etc.)
- T.O.E (Target of Evaluation) : une cible
- Vulnérabilité : une faiblesse dans le système (p. ex., mures en bois)
- Exploit : Une procédure (les étapes et les outils) permettant à une menace d'exploiter une vulnérabilité sur un T.O.E

Footprinting : ramasser, d'une manière "non intrusive", le maximum d'information sur la cible dans le but de découvrir ses vulnérabilités

# Objectif du footprinting

Pour l'attaquant, cela permet de mieux connaître la cible. Pour l'administrateur de sécurité, cela permet de comprendre ce que les autres connaissent sur son système. Faites-le avant l'attaquant !

## Objectif

- ➔ Rassembler, sans contact "intrusif", le maximum d'informations sur la cible incluant :
  - Le domaine, les emplacements physiques, les contacts (noms de personnes, téléphones, adresses courriel).
  - Les intervalles des adresses IP, les masques des sous-réseaux.
  - Etc.

## Remarque :

Wn moyenne un attaquant passe 90% de son temps à faire la reconnaissance et 10% à lancer l'attaque

# Objectif du footprinting

Remarques :

- ▶ Le piratage est toujours illégal et répréhensible par la loi, et ce, même si l'intention derrière cette activité n'est pas malhonnête.
- ▶ Les pirates sont souvent paranoïaques par rapport aux traces qu'ils laissent derrière eux.
- ▶ Ils veulent rester anonymes en passant par un proxy comme TOR ou son alternative JonDonym (JAP)
- ▶ Ils se procurent des cartes SIM "anonymes".
- ▶ Ils passent souvent par des adresses publiques et changent souvent d'adresse pour éviter d'être bloqués par des outils comme **fail2ban**.
- ▶ **fail2ban** : analyse le fichier log à la recherche de comportements suspects (plusieurs tentatives de mots de passe erronés, etc.). Il peut ensuite demander au pare-feu de bloquer une adresse.

*Une attaque réussite est une attaque qui atteint son objectif sans la possibilité de remonté à l'assaillant*

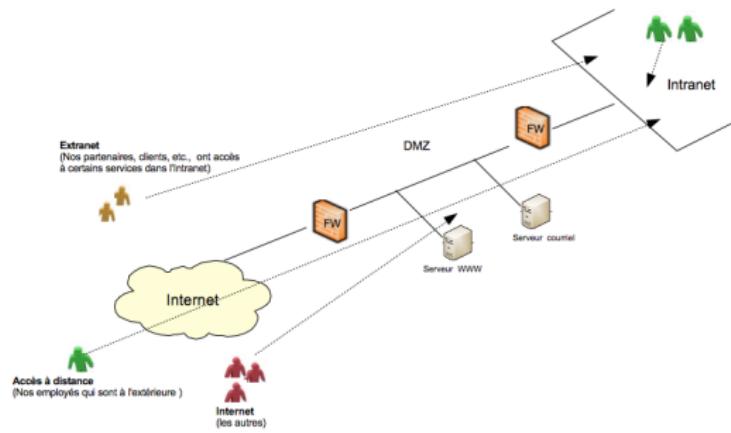
# Objectif du footprinting

Exemples d'information à collecter :

Information sur le réseau	Information sur les systèmes	Information sur l'organisation
<ul style="list-style-type: none"><li>» Noms des domaines</li><li>» Adresses IP</li><li>» Tables de routages</li><li>» Services TCP et UDP</li><li>» Protocoles Internet</li><li>» Points d'accès VPN</li><li>» Numéros de téléphones analogiques et digitales</li><li>» Mécanismes d'authentification</li><li>» ACLs</li><li>» IDS</li></ul> <p>.</p> <p>:</p>	<ul style="list-style-type: none"><li>» Noms des utilisateurs</li><li>» Mots de passe</li><li>» Noms des groupes</li><li>» Bannières de systèmes</li><li>» Information SNMP</li><li>» Architectures de systèmes</li></ul> <p>:</p>	<ul style="list-style-type: none"><li>» Détails sur les employés</li><li>» Sites web</li><li>» Répertoires de la compagnie</li><li>» Adresses physiques</li><li>» Téléphones des employés</li><li>» Nouvelles économiques</li></ul> <p>:</p>

# Informations ciblées durant un footprinting

Généralement, le réseau d'une entreprise est composé de différentes zones ayant des accès différents : Internet, Extranet, Intranet, etc.



# Informations ciblées durant un footprinting

## Internet, Intranet, Extranet

- Noms de domaines
- Blocs d'adresses IP
- Adresses des machines accessibles via Internet
- Architectures de ces machines (x86 vs sparc)
- Services TCP et UDP qui tournent sur ces machines
- Mécanismes et les listes de contrôle d'accès (ACLs)
- Systèmes de détection d'intrusions
- Énumération de systèmes (noms et groupes d'utilisateurs, bannières de systèmes, tables de routage, serveur SNMP, etc.)

# Informations ciblées durant un footprinting

## Extranet

- Origines et destinations des connexions
- Types de connections
- Mécanismes de contrôle d'accès

## Accès distants

- Numéros de téléphones numériques et analogiques
- Types de systèmes distants
- Mécanismes d'authentification
- Protocoles d'accès à distance (VPN, PPTP, etc.).

# Étapes du footprinting

- ➔ Délimiter le périmètre d'activités
- ➔ Obtenir une autorisation
- ➔ Information disponible publiquement
- ➔ Consulter l'annuaire WHOIS
- ➔ Interroger les DNSs
- ➔ Découvrir le réseau

# Étapes du footprinting

## Pentester

- Un hacker qui a voulu faire de sa passion, un métier
- Il fait des tests de pénétration (audit) pour révéler des problèmes liés à la sécurité
- Il fait des audits *black-box*, *gray-box*, *white box*, *blind*, *double blind*, etc.  
Dépendamment des informations fournies et du personnel informé
- Il suit des méthodologies de références telles que OSSTMM (Open Source Security Testing Methodology Manual) et OWASP (Open Web Application Security Project)
- Il utilise des outils de reporting (générer et partager des rapport) tels que ORC (OWASP Report Generator) et Dradis framework.
- La collecte d'information peut se faire d'une manière passive (*footprinting*) ou d'une manière active *fingerprinting*

# Délimiter le périmètre d'activités

- Toute l'entreprise
- Uniquement une sous-partie
- Connections des partenaires (Extranet)
- Sites de recouvrement de désastres
- Etc.

# Obtenir une autorisation

- L'autorisation doit être écrite et officielle
- Vous risquez la prison même si vous avez une autorisation verbale
- Elle doit couvrir et détailler toutes les activités visées
- Les criminels "oublient" cette étape

Remarque : le rapport du test de pénétration doit rester confidentiel, car il peut révéler certaines vulnérabilités

# Information disponibles publiquement

- Site web de la compagnie
- Organisations liées à la cible
- Emplacements physiques
- Employés : noms, téléphones, courriels, vies privées, anciens employés, employés expulsés, etc.
- Nouvelles économiques : acquisitions, fusions, réduction d'activités, fermetures, etc.
- Technologies

# Information disponibles publiquement

## Site web

- Réviser le contenu : le site web peut donner une quantité excessive d'information : nouveaux matériels de sécurité, nouvelles techniques de contrôle d'accès, fusions avec d'autres compagnies, acquisitions d'autres compagnies, etc.

"We are proud to have just updated all of our Cobalt servers to Plesk7 Virtual Site Servers. Anyone logging in to these new servers as admin should use the username of the domain, for example, www.xyz.com. The passwords have been transferred from the old servers, so no password reset should be required. We used the existing domain administrator password. Our continued alliance with Enterasys has allowed us to complete our transition from Cisco equipment. These upgrades, along with our addition of a third connection to the Internet, give us a high degree of fault tolerance."

- Voir le code source des pages web : certaines informations pertinentes (noms de personnes, systèmes d'exploitation, techniques de contrôle d'accès, les noms et les adresses de partenaires, etc.) sont dans les commentaires (non visibles sur la page)

# Information disponibles publiquement

## Site web

- Même si les informations "dangereuses" ont été enlevées du site web, elles peuvent être souvent retrouvées via des sites d'archives comme :  
<http://www.archive.org/>

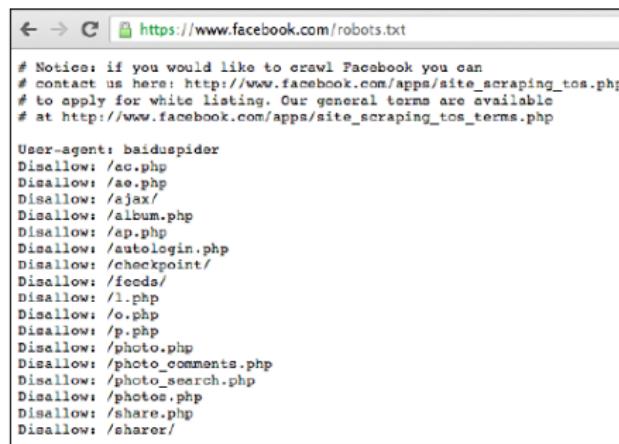
The screenshot shows the Internet Archive's Wayback Machine interface. At the top, there are links for Web, Moving Images, Texts, Audio, Software, Patron Info, About IA, and Projects. A search bar is present with a dropdown menu set to 'All Media Types'. Below the search bar, there's a section titled 'Announcements (1 item)' with a link to 'A Future for Books: BookServer launch event'. The main area is titled 'Web' and features a large image of the Parthenon. A search bar with 'Take Me Back' and 'Advanced Search' buttons is at the top right. To the right, there's a sidebar for 'Anonymous User' with options to 'Logout' or 'Upload'. The sidebar also includes a 'Welcome to the Archive' message and a 'RSS' feed link. The bottom of the page has a footer with links to various sections like 'About', 'Help', 'Contact', 'Privacy', 'Terms of Service', and 'Feedback'.

1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
0 pages	2 pages	19 pages	103 pages	263 pages	139 pages	28 pages	146 pages	304 pages	152 pages
Dec 05, 1998	• Jan 17, 1999	• Feb 29, 2000	• Jan 03, 2001	• Jan 21, 2002	• Jan 30, 2003	• Feb 09, 2004	• Jan 04, 2005	• Jan 01, 2006	•
Dec 12, 1998	• Jan 25, 1999	• Mar 01, 2000	• Jan 03, 2001	• Jan 25, 2002	• Feb 06, 2003	• Feb 09, 2004	• Jan 10, 2005	• Jan 01, 2006	•
	• Feb 03, 1999	• Mar 02, 2000	• Jan 04, 2001	• Jan 27, 2002	• Feb 20, 2003	• Mar 25, 2004	• Jan 15, 2005	• Jan 01, 2006	•
	• Feb 08, 1999	• Mar 02, 2000	• Jan 05, 2001	• Jun 03, 2002	• Mar 21, 2003	• Apr 01, 2004	• Jan 16, 2005	• Jan 01, 2006	•
	• Feb 18, 1999	• Mar 02, 2000	• Jan 06, 2001	• Jun 04, 2002	• Mar 24, 2003	• Apr 10, 2004	• Jan 18, 2005	• Jan 01, 2006	•
	• Feb 22, 1999	• Mar 03, 2000	• Jan 06, 2001	• Jun 05, 2002	• Mar 26, 2003	• Apr 15, 2004	• Jan 20, 2005	• Jan 01, 2006	•
	• Feb 23, 1999	• Mar 03, 2000	• Jan 07, 2001	• Jul 01, 2002	• Apr 11, 2003	• Apr 18, 2004	• Jan 21, 2005	• Jan 02, 2006	•
	• Apr 22, 1999	• Mar 04, 2000	• Jan 08, 2001	• Jul 02, 2002	• May 06, 2003	• May 18, 2004	• Jan 22, 2005	• Jan 02, 2006	•
	• Apr 23, 1999	• Apr 07, 2000	• Jan 08, 2001	• Jul 03, 2002	• May 13, 2003	• May 22, 2004	• Jan 24, 2005	• Jan 02, 2006	•
	• Apr 28, 1999	• Apr 09, 2000	• Jan 08, 2001	• Jul 04, 2002	• May 29, 2003	• May 26, 2004	• Jan 25, 2005	• Jan 02, 2006	•
	• Apr 29, 1999	• May 10, 2000	• Jan 08, 2001	• Jul 04, 2002	• Jun 18, 2003	• Jun 08, 2004	• Jan 27, 2005	• Jan 02, 2006	•
	• May 01, 1999	• May 10, 2000	• Jan 18, 2001	• Jul 07, 2002	• Jun 19, 2003	• Jun 09, 2004	• Jan 29, 2005	• Jan 03, 2006	•
	• May 06, 1999	• May 10, 2000	• Jan 18, 2001	• Jul 08, 2002	• Jun 23, 2003	• Jun 10, 2004	• Jan 29, 2005	• Jan 03, 2006	•
	• Oct 04, 1999	• May 11, 2000	• Jan 30, 2001	• Jul 09, 2002	• Jun 24, 2003	• Jun 10, 2004	• Jan 30, 2005	• Jan 03, 2006	•
	• Oct 07, 1999	• May 11, 2000	• Feb 02, 2001	• Jul 11, 2002	• Jul 17, 2003	• Jun 17, 2004	• Jan 31, 2005	• Jan 04, 2006	•

# Information disponibles publiquement

## Site web

- Visualiser le fichier « robots.txt » (sur la racine du site web) et visiter les liens « disallow »



```
# Notice: if you would like to crawl Facebook you can
# contact us here: http://www.facebook.com/apps/site_scraping_tos.php
# to apply for white listing. Our general terms are available
# at http://www.facebook.com/apps/site_scraping_tos_terms.php

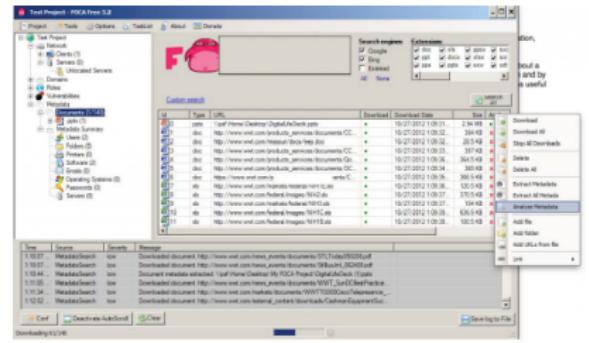
User-agent: baiduspider
Disallow: /ac.php
Disallow: /ao.php
Disallow: /ajax/
Disallow: /album.php
Disallow: /ap.php
Disallow: /autoLogin.php
Disallow: /checkpoint/
Disallow: /feeds/
Disallow: /l.php
Disallow: /o.php
Disallow: /p.php
Disallow: /photo.php
Disallow: /photo_comments.php
Disallow: /photo_search.php
Disallow: /photos.php
Disallow: /share.php
Disallow: /sharor/
```

source : web penetration testing with kali linux

# Information disponibles publiquement

## Site web

- ⇒ Les métadonnées : à chaque fois qu'on crée un document (.doc, .pdf, .xls, etc.) d'autres données seront ajoutées :
  - le nom de l'utilisateur qui a créé le document
  - le logiciel qui a créé le document
  - le nom du système d'exploitation sur lequel le document a été créé
- ⇒ Un outil comme **FOCA** peut parcourir un site web à la recherche de métadonnées dans les fichiers qu'il trouve.



source : web penetration testing with kali linux

# Information disponibles publiquement

## Site web

- ➔ Faire une copie miroir du site pour faciliter et accélérer l'analyse
  - Teleport (<http://www.tenmax.com>) pour Windows
  - Wget (<http://www.gnu.org/software/wget/>) Unix
  - HTTPTTrack (<http://www.httrack.com>) Unix, Windows, Mac
- ➔ Chercher et analyser des sites autres que `http://www` et `https/www` :
  - Outlook Web access :
    - ★ `https://owa.exemple.com`
    - ★ `https://outlook.exemple.com`
  - VPN (Virtual Private Network) :
    - ★ `http://vpn.exemple.com`
    - ★ `https://vpn.exemple.com`
- ➔ Remarque : avec certains serveurs web mal configurés, si on ne met pas le nom `index.htm`, il nous affiche le contenu de répertoire du site et il nous permettrait d'y naviguer librement

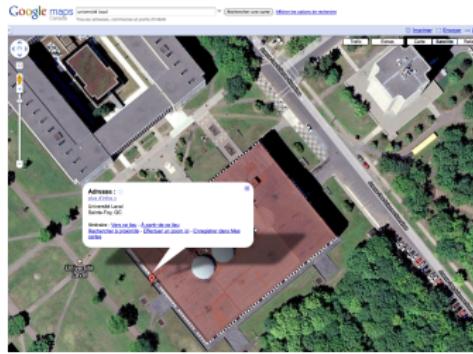
# Information disponibles publiquement

**Organisations liées à la cible** Repérer les sites qui ont un lien de, ou vers, la cible.

- ➔ Les partenaires peuvent parfois révéler des informations sensitives (technologie, etc.) sur la cible
- ➔ Si par exemple, une autre compagnie révèle qu'elle a développé le site web de la cible, alors elle-même deviendrait une cible. Elle peut par exemple nous fournir des informations sur le type de serveur web de la cible
- ➔ Un outil comme `bile.pl` permet de découvrir les sites qui sont pointés par (ou qui pointe vers) un autre  
`perl bile.pl www.exemple.ca output.txt`
- ➔ Un outil comme `bile-weigh.pl` permet d'analyser le résultat de `bile.pl` pour trouver les sites le plus significatifs

# Information disponibles publiquement

**Localisations physiques** L'@ physique est une information très pertinente

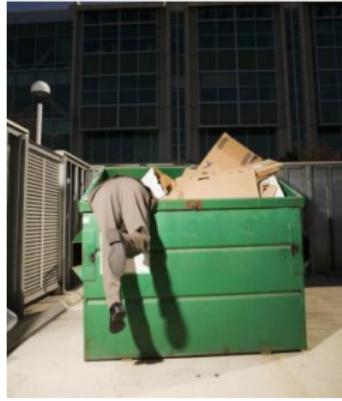


- ➔ Accès non autorisé à l'immeuble
- ➔ Mener des attaques non techniques : feux, etc.
- ➔ Accès au réseau sans fil et possiblement au réseau filaire.

# Information disponibles publiquement

## Localisations physiques

- Poubelle



<http://dedoc.ch/destruction-documents-confidentiels>

- Ingénierie sociale : connaitre les employés, avoir des amis, etc.

# Information disponibles publiquement

## Employés

- À partir d'un numéro de téléphone, trouver l'@ physique, le nom, etc.

 **PagesJaunes.ca**

[Entreprise](#) [Personne](#) [Aide](#) | [English](#)

recherche par n° de téléphone | proximité | carte | itinéraire

**quoi?\***  Nom d'entreprise seulement

Ex.: Nom d'entreprise, mot-clé, catégorie, marque,  
n° de téléphone 

**où?**  
  
Ex.: Ville, code postal, point d'intérêt 

**trouver.**

\*champ obligatoire

# Information disponibles publiquement

## Employés

- À partir de numéro de téléphone, faire l'ingénierie sociale
- À partir de l'@ physique, attaquer l'employé chez lui : voler son portable, installer un *keylogger* sur sa machine, etc.
- Les noms sont utiles pour trouver la logique de construction des adresses courriel et des noms d'utilisateurs (facilite les attaques par dictionnaire) : Pour John Smith, essayer :
  - Jsmith
  - JohnSmith
  - John.Smith
  - John\_Smith
  - jsmith@example.com

# Information disponibles publiquement

**Employés** autres informations utiles sur les employés peuvent être trouvées sur :

- ➔ un site de réseau social, professionnel, de recherche d'emploi, etc. : *facebook*, *myspace*, *jobboom*, *jobboom*, etc. En surveillant les employés sur ces sites on peut avoir des informations sur leurs mouvements, leurs expertises et parfois même certaines informations privées (date de naissance : utiliser pour s'authentifier par téléphone par des banques, des fournisseurs de services, etc.) (voir ce cas réel <http://www.le-tigre.net/Marc-L.html>)
- ➔ un site payant comme <http://www.peoplesearch.com/> qui peut donner des informations comme : numéro de tél., @, numéro d'assurance sociale, antécédent criminel, historique de crédits, etc.



Essayez de connaître même les noms des chats, des chiens, de acteurs préférés, chanteurs préférés, films préférés, noms des enfants, etc. Le mot de passe d'un employé pourrait être extrait de ces noms

# Information disponibles publiquement

**Nouvelles** bonnes nouvelles, mauvaises nouvelles, on en profite.

- fusion, acquisition, scandales, pertes, recrutement massif ou urgent, réorganisation, appel intensif à des travailleurs autonomes ou externes, etc. : Ces événements peuvent révéler des informations ou créer des opportunités et des situations propices pour l'intrus :
- Tenter de travailler ou de faire un stage à l'intérieur de la cible.

# Information disponibles publiquement

**Nouvelles** bonnes nouvelles, mauvaises nouvelles, on en profite.

- Lors d'une acquisition ou d'une fusion, le plus important est de lier les deux entités ensemble et la sécurité vient après : souvent on entend des phrases du genre « je sais que ce n'est pas la manière la plus sécurisée, mais cela nous permet d'avoir ce qu'on veut le plus rapidement possible et après on améliore la sécurité ». Ce moment après, souvent n'arrive jamais !
- Durant les recrutements beaucoup de nouveaux visages (potentiels futurs employés) entrent dans l'entreprise : difficile de détecter les personnes non autorisées

# Information disponibles publiquement

**Nouvelles** des nouvelles comme fusions, acquisitions et/ou réorganisations peuvent être trouvées dans :

- des sites de nouvelles économiques
- les rapports 10-Q (trimestriels) ou 10-K (annuels) des compagnies canadiennes sont disponibles sur le site SEDAR (<http://www.sedar.com/>). Voir EDGAR pour É.-U.



# Le dangereux Google

## Syntaxe

- mot1 mot2 : Retourne les pages contenant tous les mots spécifiés (insensible à la casse aux accents ou autres signes diacritiques "français = Francais")
- | : OR (mot1 | mot2 : retourne les pages contenant mot1 ou mot2)
- " " : Retourne les pages contenant une expression
- site:site0 : Limier la recherche aux pages du site site0. Remarque : site0 peut être un site ou un domaine)
- filetype:type0 : Limier la recherche aux fichiers ayant le type type0 (ex. filetype:pdf)
- - : Exclure un mot, un site, etc..  
Exemple : security -conference -site:www.owasp.org -inurl:.php
- .. : nombres dans un intervalle (exemple 50..100)

# Le dangereux Google

## Syntaxe

- intitle: mot, intext: mot, inanchor: mot, intext: mot : Restreint la recherche à une partie de la page.
- allintitle: mot1 mot2 (respectivement allintext:, etc.) : même chose que intitle: ((respectivement intext:, etc)) mais avec plusieurs mots



source : <https://www.rankya.com/google-advanced-search-query-syntax/>

- cache: : Limiter la recherche à la cache Google
- . : remplace un caractère (ex. *fire.fox* peut retourner *fire1fox*, *fireAfox*, etc.)
- \* : remplace une mot ("une \* vaut mille \*". "/admin/\*")

# Le dangereux Google

## Beaucoup d'informations très utiles

- ➔ Avec google, si un pirate pose la bonne question, il recevrait des résultats surprenants ! On peut :
  - avoir des fichiers de mots de passe
  - avoir des informations sur des serveurs
  - avoir des riches messages d'erreurs
  - accéder à des répertoires sensitives
  - connaître des points d'entrées légitimes (pages d'authentifications)
  - etc.
- ➔ Même si l'information est effacée du site original, elle peut rester dans la mémoire tampon de google
- ➔ Google peut agir comme mandataire (proxy) : en lui donnant une URL et on lui demande sa traduction, on aura l'information sans rentrer en contact avec le site web de la cible

# Le dangereux Google

## Fichiers et répertoires sensibles

- Fichiers de mots de passe disponibles sur Internet (des fois hébergés par des pirates)
- inurl :"passes" OR inurl :"passwords" OR inurl :"credentials" -exe filetype:txt @yahoo.com OR @gmail OR @hotmail

The screenshot shows a Google search results page with the following details:

- Search Query:** inurl:"passes" OR inurl:"passwords" OR inurl:"credentials" -exe filetype:txt @yahc
- Results:** Environ 1 680 résultats (0,26 secondes)
- First Result Preview:**
  - Title:** Wikispaces : Progenic ; Passwords[1].txt
  - Description:** progenic.wikispaces.com/file/...Passwords%5B1%5D.... ▾ Traduire cette page
  - Text Content:** Server Name: Test\_E0D6580E Type password: Messenger User: ladyblue2829 @hotmail.com Password: Server Name: Test\_E0D6580E Type password: ...
- Second Result Preview:**
  - Title:** password dictionary - Dazzlepod
  - Description:** dazzlepod.com/site\_media/bx/passwords.txt
  - Text Content:** # # This is a list of 2,151,220 unique ASCII passwords in sorted order according # to their native byte values using UNIX sort command. # This list (also known as ...
- Third Result Preview:**
  - Title:** public etrata/physical-gmail-alert Octocal-spinner-32 - GitHub
  - Description:** https://github.com/etrata/physical-gmail-alert/blob/master/credentials.txt ▾
  - Text Content:** physical-gmail-alert - A python script that physically with arduino alert the arrival of gmails.
- Fourth Result Preview:**
  - Title:** LOGIN=PASSWORD=<-----AyMen\_Hacker----->\_X...
  - Description:** tunisian-hacker.my3gb.com/passwords.txt
  - Text Content:** ... 8 LOGIN= 148599476@hotmail.fr PASSWORD= barca14789 ... 18 LOGIN= hidr.star@yahoo.com PASSWORD= 963214789 ...

# Le dangereux Google

## Fichiers et répertoires sensibles

- ➔ Chercher des données sensibles : *intext : classified top secret*
- ➔ Lister les répertoires d'un site web avec *intitle:index.of*
- ➔ On peut ajouter "Parent Dicrectory" pour avoir un meilleur résultat :  
"Parent Directory" *intitle:index.of*

Google

"parent directory" intitle:index.of

Recherche Environ 256 000 000 résultats (0,07 secondes)

Tout	<a href="#">Index of /banned books</a> premalal.com/banned%20books/ - Traduire cette page
Images	<a href="#">Parent Directory</a> - I - CIA Psychologic... > 15-May-2009 10:12 191K ! - Defeating Electr. > 15-May-2009 10:12 68K ! - Pay no Fine - A ..> 15-May-2009 10:12 ...
Maps	
Vidéos	<a href="#">Index of /booty!</a> paysites.mustbedestroyed.org/booty/ - Traduire cette page
Actualités	<a href="#">Parent Directory</a> , ~, Directory, ls2/, 2011-Sep-26 00:51:56, ~, Directory, ls3/, 2011-Oct-02 02:29:08, ~, Directory, updates_are_announced_here.txt, 2008-Mar-22 ...
Plus	
<b>Québec, QC</b>	<a href="#">Pb Index of (parent Directory) sur page perso [Résolu ...]</a> www.commentcamarche.net/.../affich-5956574-pb-index-of-parent-d... 4 réponses - 5 nov. 2008 Bonjour, Je vais essayer de vous expliquer mon problème. ... Bon ben j'ai trouvé toute seule... il ne fallait pas mettre de majuscule à index ...
<b>Le Web</b>	<a href="#">Télécharger sur des sites comme index of [Résolu]   CommentCaMar...</a> www.commentcamarche.net/.../affich-2803862-télécharger-sur-des-si... (-inurl:(htm html php) intitle:"index of" +last modified" +parent ... ⊕ Plus de résultats de commentcamarche.net
<b>Tous les résultats</b>	<a href="#">Index of /~sam</a> people.zoy.org/~sam/ Parent Directory, ~, [IMG], 0:20:02.jpeg, 30-Jul-2007 00:26, 22K. [IMG], 0:20:10.jpeg, 30-Jul-2007 00:26, 20K. [IMG], 0:32:11.jpeg, 30-Jul-2007 00:21, 16K. [IMG] ...
Sites avec des images	
Recherches associées	

# Le dangereux Google

## Fichiers et répertoires sensibles

- ➔ On peut cibler certain répertoire sensible tel que "admin": intitle:index.of inurl:admin
- ➔ On peut essayer "/admin/\*"

The screenshot shows a Google search results page. The search query is "intitle:index.of inurl:admin". The results are as follows:

- Index of /Admin - Free**  
oisy.free.fr/Admin/ - Traduire cette page  
Index of /Admin. Name Last modified Size Description. [DIR] Parent Directory 25-Aug-2011 20:46 . [TXT] Admin.htm 09-Mar-2002 15:44 1k [TXT] ...
- Index of /admin/**  
www.harcourt.fr/admin/  
Name, Size, Date, MIME Type .., -, Jul 26, 2008 18:14:12, Directory \_vti\_cnf/, -, Jul 26, 2008 18:14:13, Directory base.inc, 0.26 KB, Jul 20, 2005 12:07:33 ...
- Index of /admin - MIT**  
web.mit.edu/admin/ - Traduire cette page  
Index of /admin. Name Last modified Size Description. [DIR] Parent Directory 20-Jun-2009 23:36 . [DIR] lggv/ 14-Sep-1997 20:04 - [DIR] assignments/ ...
- Index of /admin - B-Blog**  
www.b-blog.fr/admin/  
Name - Last modified - Size - Description. [DIR], Parent Directory, ~, [IMG], 2-left.png, 24-Aug-2006 01:42, 1.3K. [IMG], 2-right.png, 24-Aug-2006 01:42, 1.3K. [IMG] ...
- Index of /admin/cio**  
www.ospm.fr/admin/cio/  
Name - Last modified - Size - Description. [DIR], Parent Directory, ~, [ ], Grio-June04.pdf, 29-Jun-2004 16:58, 480K. [ ], Joel.Marchand.pdf, 29-Sep-2005 14:02 ...
- Index of /admin - AtheistConnect**  
www.atheistconnect.org/admin/ - Traduire cette page  
Index of /admin. Parent Directory - Videos/ - big-prize-color.gif - images/. Apache Server at www.atheistconnect.org Port 80

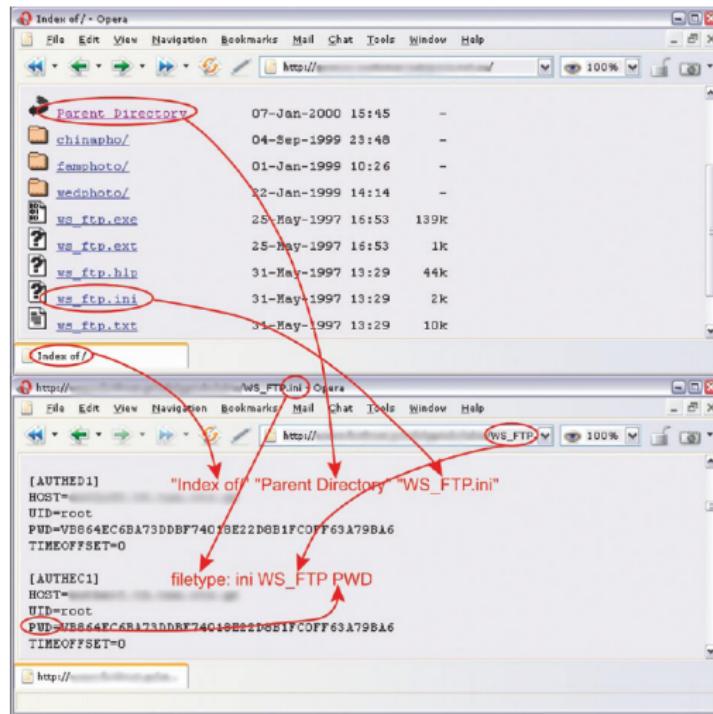
# Le dangereux Google

## Fichiers et répertoires sensibles

- ⇒ On peut cibler certain fichier sensible tel que "WS\_FTP.ini" : "WS\_FTP.ini" intitle:index.of
- ⇒ Le serveur WS\_FTP enregistre sa configuration et les mots de passe hachés de ses utilisateurs dans WS\_FTP.ini
- ⇒ D'autres informations pertinentes peuvent se trouver dans WS\_FTP.log :
  - informations sur des fichiers et des répertoires cachés
  - informations sur des noms des machines et utilisateurs qui ont fait des transferts de fichiers

# Le dangereux Google

## Fichiers et répertoires sensibles



source : [www.hakin9.org](http://www.hakin9.org)

# Le dangereux Google

## Information sensibles

- Connaitre le type et la version d'un serveur web est une information très utile pour un pirate
- On peut la trouver via la requête "Server at" intitle:index.of

Index of /raportit

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	17-Feb-2005 16:49	-	
<a href="#">2000-2001/</a>	28-Oct-2004 14:20	-	
<a href="#">2001-2002/</a>	28-Oct-2004 12:22	-	
<a href="#">2002-2003/</a>	28-Oct-2004 10:09	-	
<a href="#">2003-2004/</a>	28-Oct-2004 22:45	-	
<a href="#">2004-2005/</a>	06-Feb-2005 22:58	-	
<a href="#">images/</a>	06-Jun-2003 21:16	-	

Microsoft-IIS/5.0 Server at ... Port 80  
"Microsoft-IIS/5.0 Server at" intitle:index.of

Index of /raportit

# Le dangereux Google

## Information sensibles

- Trouver le type de serveur web en cherchant leurs pages par défaut :

- plusieurs serveurs web arrivent avec une page par défaut permettant aux administrateurs de voir que l'installation s'est bien déroulée
- ces pages, une fois indexées par Google, peuvent rester, à vie, dans sa mémoire cache
- elles peuvent même donner la configuration du serveur web
- exemples des requêtes permettant de les trouver :
  - intitle:"welcome to IIS"
  - intitle:"it worked! the apache web server"

# Le dangereux Google

## Information sensibles

- Pages de *login* (*logon*, *sign in*, etc.) peuvent être très instructives en donnant des informations comme :

- Noms de serveurs et de systèmes d'exploitation
- Procédure décrivant quoi faire si on a oublié notre mot de passe (ce point peut être le maillon faible de l'authentification)
- Noms de personnes techniques, leurs courriels, leurs numéros de téléphones, etc. à contacter en cas de problèmes
- ce qu'il arrive lorsqu'on se trompe plusieurs fois dans la saisie de mots de passe : politique de création de mots de passe

Google

login | logon

Recherche Environ 5 340 000 000 résultats (0,20 secondes)

Tout Conseil : Recherchez des résultats uniquement en français. Vous pouvez indiquer votre langue de recherche sur la page Préférences.

Images

Maps

Vidéos

Actualités

Plus

[Log in | Facebook](#)  
www.facebook.com/login.php - Traduire cette page  
- Bloquer tous les résultats de www.facebook.com  
Facebook is a social utility that connects people with friends and others who work, study and live around them. People use Facebook to keep up with friends, ...  
Facebook - Facebook Login - Sign up for Facebook - Forgotten your password?

[Sign In](#)  
www.hotmail.com/ - Traduire cette page  
Powerful free e-mail with security from Microsoft - Windows Live Hotmail is a best in class e-mail service that helps you organize and manage all your online stuff...

# Le dangereux Google

## Information sensibles

- Noms des utilisateurs (moitié de l'authentification) :

UserName | UserID | EmployeeID site: www.exemple.com

- Mots de passe (l'autre moitié) :

passwd | passcode site: www.exemple.com

- Administrateurs (leurs pages d'administration, leurs informations de contact, etc.) :

admin | administrator | admin login site: www.exemple.com

- Exclure certains types de fichiers durant la recherche :

passwd | passcode -ext:htm -ext: html site: www.exemple.com

# Le dangereux Google

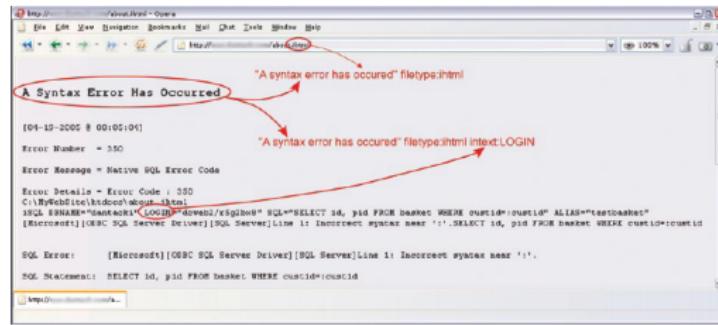
## Information sensibles

- Utiliser de l'incrémentation pour trouver d'autres informations :
  - si le répertoire `www.exemple/r1/data` existe pourquoi pas aussi `www.exemple/r2/data`
  - si le fichier `www.exemple/file1.xsl` existe pourquoi pas aussi `www.exemple/file2.xsl`
- Les fichiers du code source d'un site web ne devront pas être publics : parfois, on les trouve dans des fichiers ".bak" : `index.php.bak intitle: index.of`

# Le dangereux Google

## Les erreurs

- Les messages d'erreurs sont souvent riches en informations : types de systèmes d'exploitation, leurs configurations, noms et mots de passe d'utilisateurs, applications, structure de la base de données, etc.
- Le numéro et les messages d'erreurs peuvent révéler les types de serveurs (les erreurs HTTP de IIS sont différentes de Apache)
- Pour une base de données de type Informix, une requête comme "A syntax error has occurred" filetype:ihtml peut être très informative



source : [www.hakin9.org](http://www.hakin9.org)

# Le dangereux Google

## Les erreurs

- Pour une base de données de type MySQL, une requête comme "Access denied for user" "using password" peut être très informative

source : [www.hakin9.org](http://www.hakin9.org)

# Le dangereux Google

## Les vulnérabilités connues

- ➔ Chercher des logiciels ou des matériels connus par des vulnérabilités et des victimes potentielles
- ➔ Mots de passe pour des applications ou des équipements (routeur, commutateur, pare-feux, etc.) : Mots de passe par défaut, des comptes oubliés après la programmation, des comptes laissés par des programmeurs malsains, des backdoors laissés par le vendeur pour dépanner ses clients, etc.
- ➔ Utiliser un scanneur CGI : il cherche sur internet des fichiers CGI ayant de problèmes de sécurité connus (`userreg.cgi` permet à un pirate d'exécuter des commandes via un Shell). Nikto est un scanneur de serveur web (Open Source) connaissant 3500 fichiers CGI potentiellement dangereux, liés à une variété de serveurs et de versions.  
`inurl:/cgi-bin/userreg.cgi`

# Le dangereux Google

## Des caméra accessibles via Internet

• intitle:"Netcam" intitle:"user login"

The screenshot shows a Google search results page with the following details:

- Search Query:** intitle:"Netcam" intitle:"user login"
- Results Type:** Web
- Number of Results:** 5 résultats (0,16 secondes)
- First Result:**
  - Title:** NetCam User Login
  - Link:** 64.83.239.119/
  - Description:** User Login Page, Lite Viewer, Full Viewer, Server-Push Viewer, Administration, Plug-in · Help · Version, Name : Password :
- Second Result:**
  - Title:** NetCam User Login
  - Link:** 4.78.0.75/
  - Description:** User Login Page, Lite Viewer, Full Viewer, Server-Push Viewer, Home Page, Java Applet Viewer, Administration, Plug-in · Help · Version, Name : Password :
- Third Result:**
  - Title:** intitle:"Netcam" intitle:"user login" - Exploit Database
  - Link:** www.exploit-db.com/gdb/1151/
  - Description:** GHDB, intitle:"Netcam" intitle:"user login", prev · next, Google search: intitle:" Netcam" intitle:"user login", Hits: 2430, Submitted: 2005-09-26, just yet other online ...
- Fourth Result:**
  - Title:** User login - Công ty CP NetCam Việt Nam
  - Link:** netcamvietnam.com/index.php/joomla.../user-login
  - Description:** NETCAM VIỆT NAM Tư vấn · Lắp đặt · Sửa chữa Camera chuyên nghiệp · Trang Chủ · Tin tức · Sản phẩm · Camera Dome · Giải Pháp Camera · Camera hộ già ...

# Le dangereux Google

Trouver des systèmes Netbotz : utilisé pour surveiller température, humidité, etc. + caméra dans salle de serveurs.

→ intitle:"netbotz appliance" -inurl:.php -inurl:.asp -inurl:.pdf  
-inurl:securitypipeline -announces

Google intitle:"netbotz appliance" -inurl:.php -inurl:.asp -inurl:.pdf -inurl:securitypipeline -announces

Web Images Maps Plus Outils de recherche

Environ 2 690 résultats (0,22 secondes)

[NetBotz Appliance Software – Intrusion Detection Software | APC](#)  
www.apc.com/products/family/?id=401 ▾ Traduire cette page  
NetBotz software is designed to expand the remote management capabilities of NetBotz appliances making surveillance and intrusion detection easier than ...

[NetBotz Appliance Netbotz Rack Monitor 550 - \(NetbotzRack550\)](#)  
159.215.9.11/ ▾ Traduire cette page  
Alerting Sensors · Security Sensors · Netbotz Rack Monitor 550 · Sensor Pod ( integrated ) · testdrive door · testdrive racks · Inside corner · Over Door.

[Only one NetBotz appliance at a time can monitor a Pelco Camera ...](#)  
www.schneider-electric.us/support/index?... ▾ Traduire cette page  
Issue: When more than one NetBotz appliance monitors the same Pelco camera, Pelco camera event notifications and motion detection seem to intermi...

# Le dangereux Google

## Outils

- Des sites montrant une collection de requêtes fructueuses : [www.exploit-db.com](http://www.exploit-db.com)
- Des outils qui automatisent plusieurs requêtes : SiteDigger, gooscan, goolink scanner, goolag, etc.

Latest Google Hacking Entries		
Date	Title	Category
2011-10-11	intitle:#k4raeL - sh3LL	Vulnerable Servers
2011-10-11	filetype:php~ (pass passwd password dbpass db_pass...)	Files containing passwords
2011-09-26	+intext:"AWSTATS DATA FILE" filetype:txt	Files containing juicy info
2011-09-26	inurl:ftp "password" filetype:xls	Files containing passwords
2011-09-26	inurl:view.php?board1_sn=	Vulnerable Servers
2011-09-26	inurl:"amfphp/browser/servicebrowser.swf"...	Footholds
2011-09-12	"Powered by SLAED CMS"	Advisories and Vulnerabilities
2011-08-25	allinurl:forcedownload.php?file=	Vulnerable Files
2011-08-25	filetype:ini "Bootstrap.php" (pass passw...)	Files containing juicy info
2011-08-06	intitle:"vtiger CRM 5 - Commercial Open Sourc...	Advisories and Vulnerabilities

# Information disponibles publiquement

## Contre mesures

- Évaluer l'impact, sur la sécurité, d'une information avant de la rendre publique
- Périodiquement, évaluer les informations disponibles publiquement
- Enlever, quand cela est possible, les informations sensibles
- RFC 2196 - Security Handbook (<http://www.faqs.org/rfcs/rfc2196.html>) donne, entre autres, des règles de bonnes pratiques relatives à ce sujet

# Consulter l'annuaire Whois

Qui se cache derrière la cible ?

## WHOIS

- Annuaire mondial dans lequel se trouvent des informations sur les domaines inscrits
  - Les intervalles d'@ IP
  - Les noms de domaines
  - Points de contacts (les individus, les numéros de téléphones, courriels, adresses physiques)
  - Correspondance entre noms de machines et @IP
  - Etc.

Pour mieux comprendre cet annuaire, nous avons besoin de connaître comment certains aspects d'Internet sont gérés

# L'annuaire Whois

Qui gère Internet ? Il faut qu'il y ait une gestion globale pour, entre autres, éviter les conflits dans les attributions des adresses et des noms

- ➔ Qui a donné le nom de domaine ulaval.ca à l'université Laval ?
- ➔ Qui lui a donné ses adresses IP ?
- ➔ Qui a choisi le port 80 pour le protocole HTTP ?

# L'annuaire Whois

## Comment sont distribuées les adresses IP ?

- ➔ C'est l'ICANN (Internet Corporation for Assigned Names and Numbers), un organisme international à but non lucratif qui distribue des grands blocs de @IP à des RIRs (Regional Internet Registries)
- ➔ Il y a présentement 5 RIRs : APNIC (Asia/Pacific Region), ARIN (North America and Sub-Sahara Africa), LACNIC (Latin America and some Caribbean Islands), RIPE NCC (Europe, the Middle East and Central Asia) et AfriNIC (for Africa)  
<https://www.arin.net/knowledge/rirs/ARINcountries.html>
- ➔ Les RIRs à leurs tours distribuent des sous blocs à des LIRs (Local Internet Registries) et/ou des ISP (Internet Services Providers).
- ➔ Les ISP donnent les adresses aux utilisateurs finaux.

# L'annuaire Whois



Registry	Area Covered
<a href="#">AfriNIC</a>	Africa Region
<a href="#">APNIC</a>	Asia/Pacific Region
<a href="#">ARIN</a>	North America Region
<a href="#">LACNIC</a>	Latin America and some Caribbean Islands
<a href="#">RIPE NCC</a>	Europe, the Middle East, and Central Asia

<http://www.iana.org/numbers>

# L'annuaire Whois

Comment sont attribués les domaines ?

Les gTLD (Generic Top Level Domains) sont :

.com	.coop
.net	.info
.org	.museum
.aero	.name
biz	.pro

- C'est l'ICANN qui attribue les noms de gTLD par intermédiaire de "registrars"
- Il y a présentement 467 "registrars" pour les gTLD dont 358 sont situés aux États-Unis et au Canada, 58 en Europe et 51 en Asi-Pacifique

# L'annuaire Whois

Comment sont attribués les domaines ?

Les ccTLD (Country Code Top Level Domains) : .ca, .fr, .it, .tn, ...

- Les RIRs distribuent les ccTDL associés à leurs zones géographiques.
- Le ".ca" est géré par l'ACEI (Autorité Canadienne pour les Enregistrements Internet)
- Sous-domaines : .gc.ca, .on.ca, .qc.ca, etc
- Pour enregistrer un nom de domaine "point-ca", vous devez passer par l'intermédiaire de l'un des registraires agréés : voir la liste sur [http://ro.cira.ca/re\\_choose](http://ro.cira.ca/re_choose)
- Présentement, à chaque fois qu'un registraire enregistre un domaine, il paye 8,5\$/année (source <http://www.cira.ca/comment-devenir-registraire/>)

# L'annuaire Whois

Exemple de registraires : DomainsAtCost, easyDNS, etc :

- Font les inscriptions auprès des autorités auxquelles ils sont attachés.
- Pour les Canadiens, ces autorités sont ACEI (CIRA) pour les point-ca, ou ARIN pour les autres domaines

# L'annuaire Whois

Comment procède-t-on pour avoir un nom de domaine ?

- Choisir le nom de domaine à enregistrer
- Vérifier la disponibilité à l'aide de Whois
- Remplir un formulaire (propriétaire, coordonnées, adresse courriel, contacte, facturation, un DNS primaire et un DNS secondaire qui sont donnés par l'ISP)
- Vous pouvez ne pas donner les serveurs DNS en cas où vous voulez juste enregistrer le nom pour une utilisation future.
- Coût : 10 à 50 \$ par année
- Vous aurez un compte à travers lequel vous pouvez changer ces informations
- Par exemple, si vous changez de ISP, vous changez de DNS

# L'annuaire Whois

## Remarques

- L'annuaire Whois est distribué sur plusieurs serveurs localisés dans des régions et des pays différents et gérés de manières différentes
- La syntaxe de requêtes, les types de requêtes permises, les formats et les contenus de réponses varient d'un serveur à un autre
- Certains serveurs ne permettent qu'une liste très restrictive de requêtes pour combattre le "hacking"
- Les informations Whois pour les domaines ".mil" (militaire américain) et ".gov" (gouvernements américains) ont été retirées pour des raisons de sécurité.

# L'annuaire Whois

## Comment faire la recherche à partir d'un nom de domaine ?

- ➔ Plusieurs outils sont disponibles, mais il faut de la patience, car rien ne fonctionne à 100% tout le temps
- ➔ En mode commande sous unix, il y a la fameuses commande whois
- ➔ `whois help@whois-server`  
donne la syntaxe et les requêtes permises sur le serveur en question

# L'annuaire Whois

Comment faire la recherche à partir d'un nom de domaine ? Supposons qu'on cherche "company.com"

- Généralement, trois requêtes sont nécessaires pour trouver l'information recherchée
- Le serveur whois.iana.org nous donne le responsable d'un TLD donné.  
Dans notre cas le TLD est ".com"  
`whois com@whois.iana.org`
- La réponse nous indique que le responsable du ".com" est "verisign-grs.com"  
(connu aussi par "whois.crsnic.com")
- La requête `whois company.com@whois.crsnic.org` nous donne le registraire chez qui est enregistré le domaine company.com
- La requête `whois company.com@whois.registraire.com` nous donne les informations sur le domaine "company.com"

# L'annuaire Whois

Le travail peut se faire via les sites Internet des entités impliquées



Internet Assigned Numbers Authority

The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources. [Learn more about what we do »](#)

[Domain Names](#)

IANA manages the DNS Root Zone (assignments of ccTLDs and gTLDs), as well as the .int registry, and the .arpa zone.

- [Root Zone Management](#)
- [Database of Top Level Domains](#)
- [.int Registry](#)
- [.arpa Registry](#)
- [IDN Practices Repository](#)
- [Interim Trust Anchor Repository](#)

[Number Resources](#)

IANA coordinates the global IP and AS number space, and allocates these to Regional Internet Registries.

- [IP Addresses & AS Numbers](#)
- [Think we're attacking you?](#)

[Protocol Assignments](#)

IANA is the central repository for protocol name and number registries, used in many Internet protocols.

- [Protocol Registries](#)
- [Apply for an assignment](#)

Search the site:

# L'annuaire Whois

 VeriSign

US Home | Worldwide Sites | Contact Us | Site Map

[Products & Services](#) [Partners](#) [Support](#) [About VeriSign](#) [Existing Customers](#)

**Domain Name Services**

- [Domain Name Registries](#)
- [Become a Registrar](#)
- [For Current Registrars](#)
- [Find a Registrar](#)
- [Information Center](#)
- [Whois](#)
- [Why VeriSign?](#)

US Home > Products & Services > Domain Name Services > Whois - .com, .net, .edu

## Whois - .com, .net, .edu

[.com](#) [.net](#) [.edu](#) | [.cc](#) | [.tv](#) | [.jobs](#) | [.name](#)

[Email](#) [Bookmark](#) [Print](#)

**Contact Us**

Contact Support at  
703-925-6999  
[Info@verisign-grs.com](mailto:info@verisign-grs.com)

**Search the .com, .net, .edu Whois**

By submitting a Whois query, user agrees to abide by the [Terms of Use](#).

**Search Whois For:**

Domain (ex.verisign.com)  
 Registrar (ex. ABC Registrar, Inc.)  
 Nameserver (ex.NS.VERISIGN.COM or 198.41.0.196)

[Help](#) | [FAQs](#)

**Please Note:** Successful domain registrations and modifications may not be in the WHOIS database for up to 48 hours.

[Contact Us](#) | [Careers](#) | [Legal Notices](#) | [Privacy](#) | [Repository](#) | ©1995-2009 VeriSign, Inc. All rights reserved.

# L'annuaire Whois

Registrant:  
    Dns Admin  
    Google Inc.  
    Please contact contact-admin@google.com 1600 Amphitheatre Parkway  
        Mountain View CA 94043  
        US  
        dns-admin@google.com +1.6502530000 Fax: +1.6506188571

Domain Name: google.com

Registrar Name: Markmonitor.com  
Registrar Whois: whois.markmonitor.com  
Registrar Homepage: http://www.markmonitor.com

Administrative Contact:  
    DNS Admin  
    Google Inc.  
    1600 Amphitheatre Parkway  
        Mountain View CA 94043  
        US  
        dns-admin@google.com +1.6506234000 Fax: +1.6506188571

Technical Contact, Zone Contact:  
    DNS Admin  
    Google Inc.  
    2400 E. Bayshore Pkwy  
        Mountain View CA 94043  
        US  
        dns-admin@google.com +1.6503300100 Fax: +1.6506181499

Created on.....: 1997-09-15.  
Expires on.....: 2011-09-13.  
Record last updated on..: 2009-06-21.

Domain servers in listed order:

ns2.google.com  
ns4.google.com  
ns1.google.com  
ns1.google.com

# L'annuaire Whois

Certains outils font tout le travail via une seule requête : [www.uwhois.com](http://www.uwhois.com), [www.allwhois.com](http://www.allwhois.com), [www.gektools.com](http://www.gektools.com), etc.

**Uwhois.com**  
THE UNIVERSAL "WHO IS" FOR INTERNET DOMAINS.

**Corporate.com**  
Incorporate your business and manage it without leaving your browser.

Home | About Uwhois | Premium Services | Free Software | Contact Us | Legal

Uwhois.com Search: Go

To identify the registered holder of a domain name, enter the domain name, followed by either .com, .net, .org, or one of the 246 country code suffixes in the entry box above and click the go button.

Financing, Payroll, Merchant services, And more.

oneCore.com

**ditto**  
Visual Search

Get what you really wanted.  
**eBay** click here

Search multiple Generic and Country Code Top Level Domains.

① Enter domain or IP then press GO!

② Site server determines which registry server to query

③ Search is performed and the result is sent back to the browser

IP Number  
domain.com  
domain.net  
domain.org  
etc.

Registry Servers

u who is.com

# L'annuaire Whois

Comment faire la recherche à partir d'une adresse IP (e.g. 61.0.0.2) ?

- Si vous connaissez le bon RIR, aller lui demander
- Sinon demander à n'importe quel RIR et s'il ne connaît pas la réponse, il vous donne le bon RIR
- Exemple `whois 61.0.0.2@whois.arin.net`

# L'annuaire Whois

Le serveur "arin.net" n'est pas le bon RIR mais il vous demande soit d'interroger whois.apnic.com soit d'aller sur le site web  
<http://wq.apnic.net/apnic-bin/whois.pl>

**ARIN WHOIS Database Search**

Relevant Links: [ARIN Home Page](#) [ARIN Site Map](#) Training: [Querying ARIN's WHOIS](#)

Search ARIN WHOIS for: 60.0.0.2

Envoyer

OrgName: Asia Pacific Network Information Centre  
OrgID: APNIC  
Address: PO Box 2131  
City: Milton  
StateProv: QLD  
PostalCode: 4064  
Country: AU

ReferralServer: whois://whois.apnic.net

NetRange: 60.0.0.0 - 60.255.255.255  
CIDR: 60.0.0.0/8  
NetName: APNIC-60  
NetHandle: NET-60-0-0-0-1  
Parent:  
NetType: Allocated to APNIC  
NameServer: NS1.APNIC.NET  
NameServer: NS3.APNIC.NET  
NameServer: NS4.APNIC.NET  
NameServer: TINNIE.ARIN.NET  
NameServer: NS2.LACNIC.NET  
NameServer: NS-SEC.RIPE.NET

Comment: This IP address range is not registered in the ARIN database.  
Comment: For details, refer to the APNIC Whois Database via  
[WHOIS.APNIC.NET](#) or <http://wq.apnic.net/apnic-bin/whois.pl>  
Comment: \*\* IMPORTANT NOTE: APNIC is the Regional Internet Registry  
Comment: for the Asia Pacific region. APNIC does not operate networks  
Comment: using this IP address range and is not able to investigate  
Comment: spam or abuse reports relating to these addresses. For more  
Comment: help, refer to [http://www.apnic.net/apnic-info/whois\\_search2/abuse-and-spamming](http://www.apnic.net/apnic-info/whois_search2/abuse-and-spamming)

# L'annuaire Whois

APNIC - Query the APNIC Whois Database

To assist you with debugging problems, this whois query was received from IP Address  
[132.203.120.16]  
Your web client may be behind a web proxy.

Search for

**IP address lookups**

- I** 1st level less specific
- L** All less specific
- m** 1st level more specific
- M** All more specific
- x** Exact match only
- d** Associated reverse domain

**Miscellaneous queries**

- i** Inverse attributes
- T** Object types

**Query hints**

- Include "AS" in front of an AS number.  
Example: AS4808
- Include "-t" (template only) or "-v" (template and description) in front of an object name to view the template  
Example: -t inetnum

For more information see:

- [Using Whois](#)
- [Report invalid contact](#)

# L'annuaire Whois

APNIC - Query the APNIC Whois Database

To assist you with debugging problems, this whois query was received from IP Address  
[132.203.120.16]  
Your web client may be behind a web proxy.

% APNIC found the following authoritative answer from: whois.apnic.net

% [whois.apnic.net node-1]  
% Whois data copyright terms <http://www.apnic.net/db/dbcopyright.html>

**inetnum:** 60.0.0.0 - 60.10.255.255  
**netname:** UNICOM-HE  
**descr:** China Unicom Hebei Province Network  
**descr:** China Unicom  
**country:** CN  
**admin-c:** CH1302-AP  
**tech-c:** KL984-AP  
**remarks:** service provider  
**mnt-by:** APNIC-HB  
**mnt-lower:** MAINT-CNCGROUP-HE  
**mnt-routes:** MAINT-CNCGROUP-RR  
**status:** ALLOCATED PORTABLE  
**remarks:** +-+---+--+---+--+---+--+---+--+---+--+---+--+---+--+---+--+---+  
**remarks:** This object can only be updated by APNIC hostmasters.  
**remarks:** To update this object, please contact APNIC  
**remarks:** hostmasters and include your organisation's account  
**remarks:** name in the subject line.  
**remarks:** +-+---+--+---+--+---+--+---+--+---+--+---+--+---+--+---+--+---+  
**changed:** hm-changed@apnic.net 20040329  
**changed:** hm-changed@apnic.net 20060113  
**changed:** hm-changed@apnic.net 20060124  
**changed:** hm-changed@apnic.net 20080314  
**changed:** hm-changed@apnic.net 20090508  
**source:** APNIC

**route:** 60.0.0.0/13  
**descr:** CNC Group CHINA169 Hebei Province Network  
**country:** CN  
**origin:** AS4837  
**mnt-by:** MAINT-CNCGROUP-RR  
**changed:** abuse@cnc-noc.net 20060118  
**source:** APNIC

# L'annuaire Whois

## Quelques outils utiles

Mechanism	Resources	Platform
Web interface	<a href="http://www.networksolutions.com/">http://www.networksolutions.com/</a>	Any platform with a web client
Web interface	<a href="http://www.arin.net/">http://www.arin.net/</a>	Any platform with a web client
Whois client	Unix; Fwhois <ccappuc@santafe.edu>	UNIX
WS Ping Pong	<a href="http://www.ipswitch.com/">http://www.ipswitch.com/</a>	Win 9x/NT
Sam Spade	<a href="http://www.blighty.com/products/spade">http://www.blighty.com/products/spade</a>	Win 9x/NT
Sam Spade Web Interface	<a href="http://www.samspade.org/">http://www.samspade.org/</a>	Any platform with a web client
Netscan tools	<a href="http://www.nwpsw.com/">http://www.nwpsw.com/</a>	Win 9x/NT
Xwhois toolkit	<a href="http://www.goatnet.ml.org/software.html">http://www.goatnet.ml.org/software.html</a>	UNIX with X and GTK+ GUI

# L'annuaire Whois

## Contre mesures

- ➔ Réviser et limiter les informations fournies à votre registraire
- ➔ Utiliser des noms de rôles (p. ex. responsable web) et jamais des noms d'individus
- ➔ Fournir vos numéros de téléphone sans frais ( 1-800-...) et non pas des numéros de lignes directes pour éviter le "war-dialing"

# Interroger les DNSs

Rappel :

- ➔ Pourquoi a-t-on besoin des noms alors que les ordinateurs utilisent les adresses IP ?
  - les noms sont plus faciles à mémoriser
  - en changeant un ordinateur d'un réseau à un autre, les adresses IP changent
- ➔ Au tout début, les correspondances entre les noms et les adresses IP sont enregistrées dans un fichier local. Cette fonctionnalité existe encore
  - c:\windows\system32\drivers\etc\hosts (Windows)
  - /etc/hosts (Unix)

# Interroger les DNSs

Rappel : problèmes liés à l'utilisation d'un fichier local

- > Le fichier est volumineux
- > Il doit être copié fréquemment sur toutes les machines
- > Problème d'unicité de noms
- > Pas approprié à grande échelle
- > Pour résoudre ces problèmes, on a créé le DNS (Domain Name System) défini dans RFC 1034 et 1035.

# Interroger les DNSs

Rappel : l'espace de noms

- Le fondement est basé sur un schéma de nommage hiérarchique (les domaines) et une base de données répartie

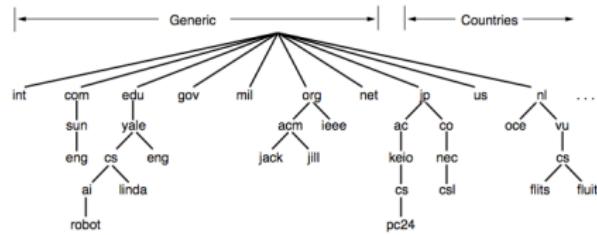


Fig. 7-1. A portion of the Internet domain name space.

source : livre Réseaux 4/e de A. Tanenbaum

# Interroger les DNSs

Rappel : l'espace de noms

- Il est divisé en **zones**
- Une zone peut contenir plusieurs niveaux de l'arbre mais elle doit être continue
- Chaque zone contient des serveurs (1 primaire et 1 ou plusieurs secondaires) de noms contenant les informations relatives à sa zone

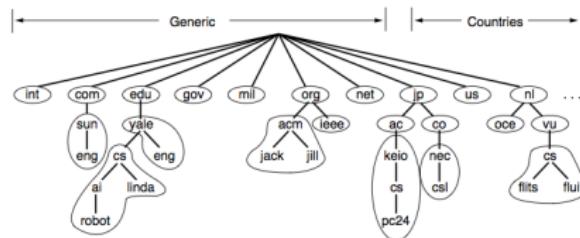


Fig. 7-4. Part of the DNS name space showing the division into zones.

source : livre Réseaux 4/e de A. Tanenbaum

# Interroger les DNSs

Rappel : contenu des enregistrements de la base de données DNS

- Chaque ligne a le format suivant :  
Nom Durée\_de\_vie Classe Type Valeur
- Classe : souvent IN (Internet), on peut aussi trouver CH qui donne la version du serveur DNS lui même (ex. version.bind. 0 CH TXT "9.6.2-P3")
- À un seul domaine peut correspondre plusieurs lignes

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

Fig. 7-2. The principal DNS resource record types for IPv4.

source : livre Réseaux 4/e de A. Tanenbaum

# Interroger les DNSs

Rappel : contenu des enregistrements de la base de données DNS

• Le premier enregistrement doit être de type SOA et donne les informations suivantes :

```
@ IN SOA      nameserver.place.dom. postmaster.place.dom. (
                      1           ; serial number
                      3600        ; refresh   [1h]
                      600         ; retry     [10m]
                     86400       ; expire    [1d]
                     3600 )      ; min TTL  [1h]
```

- ▶ Origine : le nom du serveur primaire (ex. nameserver.place.dom)
- ▶ Contact : l'@ courriel de la personne chargée d'administrer la zone. Le premier point dans l'adresse doit être suivi de "@" (ex. postmaster@place.dom)
- ▶ Numéro de série : incrémenté de un à chaque fois le fichier est modifié. Cela aide les serveurs secondaires à savoir s'il y a de changements avant de faire le transfert. Donne aussi le nombre de fois de modification de fichier
- ▶ Temps de rafraîchissement : temps (en secondes) que les serveurs secondaires doivent attendre avant de redemander l'enregistrement SOA
- ▶ Temps de réessayage : temps (en secondes) qu'un serveur secondaire doit attendre, en cas de problèmes durant le transfert de données, avant de réessayer
- ▶ Expiration : Si un serveur secondaire n'arrive pas à se rafraîchir avant cette durée (en secondes), il considère que ses données sont "périmentées" et il ne répond plus à des requêtes DNS
- ▶ TTL : cette information est fournie dans les réponses des requêtes DNS pour gérer les mémoires caches. Si c'est zéro, donc on ne met pas l'information dans la mémoire cache.

# Interroger les DNSs

Rappel : contenu des enregistrements de la base de données DNS

- À un seul domaine peuvent correspondre plusieurs lignes

```
; Authoritative data for cs.vu.nl
cs.vu.nl.      86400  IN  SOA   star boss (9527,7200,7200,241920,86400)
cs.vu.nl.      86400  IN  TXT   "Divisie Wiskunde en Informatica."
cs.vu.nl.      86400  IN  TXT   "Vrije Universiteit Amsterdam."
cs.vu.nl.      86400  IN  MX    1 zephyr.cs.vu.nl.
cs.vu.nl.      86400  IN  MX    2 top.cs.vu.nl.

flits.cs.vu.nl. 86400  IN  HINFO Sun Unix
flits.cs.vu.nl. 86400  IN  A    130.37.16.112
flits.cs.vu.nl. 86400  IN  A    192.31.231.165
flits.cs.vu.nl. 86400  IN  MX   1 flits.cs.vu.nl.
flits.cs.vu.nl. 86400  IN  MX   2 zephyr.cs.vu.nl.
flits.cs.vu.nl. 86400  IN  MX   3 top.cs.vu.nl.
www.cs.vu.nl.   86400  IN  CNAME star.cs.vu.nl
ftp.cs.vu.nl.   86400  IN  CNAME zephyr.cs.vu.nl

rowboat          IN  A    130.37.56.201
                  IN  MX   1 rowboat
                  IN  MX   2 zephyr
                  IN  HINFO Sun Unix

little-sister    IN  A    130.37.62.23
                  IN  HINFO Mac MacOS

laserjet         IN  A    192.31.231.216
                  IN  HINFO "HP Laserjet IIISi" Proprietary
```

Fig. 7-3. A portion of a possible DNS database for *cs.vu.nl*

source : livre Réseaux 4/e de A. Tanenbaum

# Interroger les DNSs

Rappel : contenu des enregistrements de la base de données DNS

- Déléguer une zone d'un sous-domaine : si on veut mettre en place plusieurs serveurs DNS, chacun gérant sa zone correspondant à son sous-domaine. Exemple le domaine domaine1.ca veut déléguer la gestion des sous-domaines division1.domaine1.ca et division2.domaine1.ca aux serveurs de noms ns.division1.domaine1.ca (168.131.1.1) et ns.division2.domaine1.ca (168.131.2.1), il faut ajouter dans le fichier de zone de domaine1.ca les lignes suivantes :

```
;  
; Delegation des sous domaines division1.domaine1.ca et division2.domaine1.ca  
;  
division1.domaine1.ca.      IN    NS    ns.division1.domaine1.ca.  
division2.domaine1.ca.      IN    NS    ns.division2.domaine1.ca.  
  
ns.division1.domaine1.ca.  IN    A     168.131.1.1  
ns.division2.domaine1.ca.  IN    A     168.131.2.1
```

Ne pas oublier aussi de mettre à jour le fichier de résolution inverse domaine1.ca.rev

```
;  
; Delegation des sous domaines division1.domaine1.ca et division2.domaine1.ca  
;  
1.132.168.in-addr.arpa.  IN    NS    ns.division1.domaine1.ca.  
2.131.168.in-addr.arpa.  IN    NS    ns.division2.domaine1.ca.
```

# Interroger les DNSs

Rappel : Installer un serveur DNS : comment on procède ?

♦ 1) Préparation du contenu pour notre domaine (exemple : garage.ca.)

- Ce nom de domaine sera géré par deux serveurs dns :  
ns1.garage.ca - 192.168.0.1 (serveur maître);  
ns2.garage.ca - 192.168.0.2 (serveur esclave).
- Les courriels de ce domaine seront gérées par les deux serveurs suivant :  
mx1.garage.ca - 192.168.0.3;  
mx2.garage.ca - 192.168.0.4.
- Ce domaine contient trois machines :  
tuto.garage.ca - 192.168.0.5 ;  
www.garage.ca - 192.168.0.6 ;  
ftp.garage.ca - 192.168.0.7.
- La machine blog.garage.ca sera un alias de www.garage.ca.

♦ 2) installer Bind9

```
# apt-get install bind9
```

# Interroger les DNSs

Rappel : Installer un serveur DNS : comment on procède ? (suite)

- 3) Créer les zones dans le fichier /etc/bind/named.conf

```
;serveur primaire
zone "garage.ca" {
    type master;                                ; Le type indique si vous êtes master ou slave sur la zone
    file "/etc/bind/dns.garage.ca";             ; Le nom de fichier dans lequel se trouvent les enregistrements DNS
    allow-transfer { 192.168.0.2; };              ; L'adresse du serveur secondaire est 192.168.0.2
};

;serveur secondaire
zone "garage.ca" {
    type slave;                                 ; Le type indique si vous êtes master ou slave sur la zone
    file "/etc/bind/dns.garage.ca";             ; Le nom de fichier dans lequel se trouvent les enregistrements DNS
    allow-transfer { 192.168.0.1; };              ; L'adresse du serveur primaire est 192.168.0.1
};

;résolution inverse

zone "0.168.192.in-addr.arpa." { ; résoudre toutes les adresses qui commencent par 192.168.0
    type master;
    file "/etc/bind/dns.192.168.0";
};
```

# Interroger les DNSs

Rappel : Installer un serveur DNS : comment on procède ? (suite)

- 3) Créer les fichiers zones dans le fichier /etc/bind/dns.garage.ca

```
@ IN SOA ns1.garage.ca. admin.garage.ca. (
    2013020905 ;serial
    3600   ; refresh (1 hour)
    3000   ; retry (50 minutes)
    86400  ; expire (1 day)
    604800 ; minimum (1 week)
)

@      IN  NS   ns1.garage.ca.
@      IN  NS   ns2
@      IN  MX   10 mx1
@      IN  MX   20 mx2
ns1    IN  A    192.168.0.1
ns2    IN  A    192.168.0.2
mx1    IN  A    192.168.0.3
mx2    IN  A    192.168.0.4
tuto   IN  A    192.168.0.5
www    IN  A    192.168.0.6
ftp    IN  A    192.168.0.7
blog   IN  CNAME www
```

# Interroger les DNSs

Rappel : Installer un serveur DNS : comment on procède ? (suite)

- 3) Créer les fichiers zones dans le fichier /etc/bind/dns.192.168.0

```
@ IN SOA ns1.garage.ca. admin.garage.ca. (
    2013020905 ;serial
    3600      ; refresh (1 hour)
    3000      ; retry (50 minutes)
    86400     ; expire (1 day)
    604800    ; minimum (1 week)
)

@ IN NS ns1.garage.ca.
@ IN NS ns2.garage.ca.
1  IN PTR ns1.garage.ca.
2  IN PTR ns2.garage.ca.
3  IN PTR mx1.garage.ca.
4  IN PTR mx1.garage.ca.
5  IN PTR tuto.garage.ca.
6  IN PTR www.garage.ca.
7  IN PTR ftp.garage.ca.
```

# Interroger les DNSs

## Rappel

- Le DNS est une application client-serveur (requêtes/réponses) port 53, protocole UDP (occasionnellement TCP, p. ex. pour les grandes requêtes >512 octets)
- L'implantation du serveur et du résolveur DNS la plus utilisée est BIND (Berkeley Internet Name Domain)

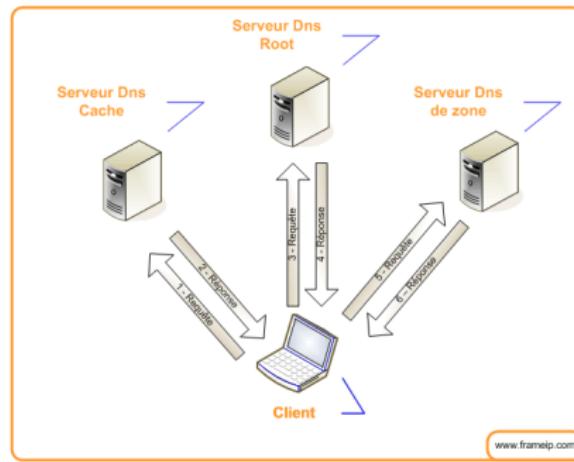
; Authoritative data for cs.vu.nl			
cs.vu.nl.	86400	IN SOA	star.boss (9527,7200,7200,241920,86400)
cs.vu.nl.	86400	IN TXT	"Divisie Wiskunde en Informatica."
cs.vu.nl.	86400	IN TXT	"Vrije Universiteit Amsterdam."
cs.vu.nl.	86400	IN MX	1 zephyr.cs.vu.nl.
cs.vu.nl.	86400	IN MX	2 top.cs.vu.nl.
flits.cs.vu.nl.	86400	IN HINFO	Sun Unix
flits.cs.vu.nl.	86400	IN A	130.37.16.112
flits.cs.vu.nl.	86400	IN A	192.31.231.165
flits.cs.vu.nl.	86400	IN MX	1 flits.cs.vu.nl.
flits.cs.vu.nl.	86400	IN MX	2 zephyr.cs.vu.nl.
flits.cs.vu.nl.	86400	IN MX	3 top.cs.vu.nl.
www.cs.vu.nl.	86400	IN CNAME	star.cs.vu.nl
ftp.cs.vu.nl.	86400	IN CNAME	zephyr.cs.vu.nl
rowboat		IN A	130.37.56.201
		IN MX	1 rowboat
		IN MX	2 zephyr
		IN HINFO	Sun Unix
little-sister		IN A	130.37.62.23
		IN HINFO	Mac MacOS
laserjet		IN A	192.31.231.216
		IN HINFO	"HP Laserjet IIISi" Proprietary

Fig. 7-3. A portion of a possible DNS database for *cs.vu.nl*

source : livre Réseaux 4/e de A. Tanenbaum

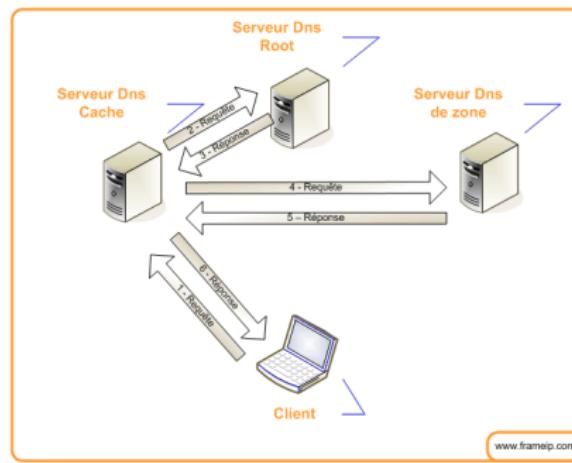
# Interroger les DNSs

Rappel : résolveur en mode itératif



# Interroger les DNSs

Rappel : résolveur en mode récursif



# Interroger les DNSs

## Rappel : OpenDNS

IPv4 : 208.67.222.222 ou 208.67.222.220 ou 208.67.220.220 ou 208.67.220.222

IPv6 : 2620:0:ccc::2 ou 2620:0:ccd::2

- ➔ Un serveur DNS ouvert au public. Il accepte n'importe quelle requête DNS
- ➔ Le trafic est protégé (chiffré par DNSCrypt) : DNSCrypt (chiffre le contenu du DNS) est différent de DNSSECURE (assure l'authentification des messages)
- ➔ Détient une liste noire de sites web
- ➔ Permet de faire un contrôle parental en configurant le DNS d'une machine ou le DNS du routeur sans fil à :  
208.67.222.123 ou 208.67.220.123
- ➔ Plusieurs l'utilisent car il offre une meilleure sécurité et fiabilité que le DNS de leurs ISP.

# Interroger les DNSs

Accéder aux contenus des enregistrements DNS : dig, host, nslookup, etc.

- dig : un programme qui fait des requêtes DNS et affiche les résultats
- dig [@Server] [query-type] [name]
  - Server est le nom ou l'@ IP du serveur à qui on envoie la requête
  - query-type est le type (A, MX, PTR, TXT, etc.) de l'enregistrement demandé (par défaut c'est "A")
  - name : cela prend différentes formes dépendamment du champ query-type nom d'un domaine, nom d'une machine, ou une @ IP (lorsque le type est PTR)

# Interroger les DNSs

Accéder aux contenus des enregistrements DNS : exemple avec dig  
dig www.google.com

```
; <>> DiG 9.6.0-APPLE-P2 <>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 53996
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;www.google.com.           IN      A
;; ANSWER SECTION:
www.google.com.      50262   IN      CNAME   www.l.google.com.
www.l.google.com.      50      IN      A       66.249.81.104
;; Query time: 2 msec
;; SERVER: 10.141.1.10#53(10.141.1.10)
;; WHEN: Sun Nov 15 21:11:24 2009
;; MSG SIZE  rcvd: 68
```

# Interroger les DNSs

Accéder aux contenus des enregistrements DNS : exemple avec dig

Les noms des serveurs courriel attachés à un domaine.

```
dig google.com mx
```

```
; <>> DiG 9.6.0-APPLE-P2 <>> google.com mx
;; global options: +cmd
;; Got answer:
;; -->HEADER<- opcode: QUERY, status: NOERROR, id: 10690
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 4

;; QUESTION SECTION:
;google.com.           IN      MX

;; ANSWER SECTION:
google.com.        900     IN      MX      10 google.com.s9a2.psmtp.com.
google.com.        900     IN      MX      10 google.com.s9b1.psmtp.com.
google.com.        900     IN      MX      10 google.com.s9b2.psmtp.com.
google.com.        900     IN      MX      10 google.com.s9a1.psmtp.com.

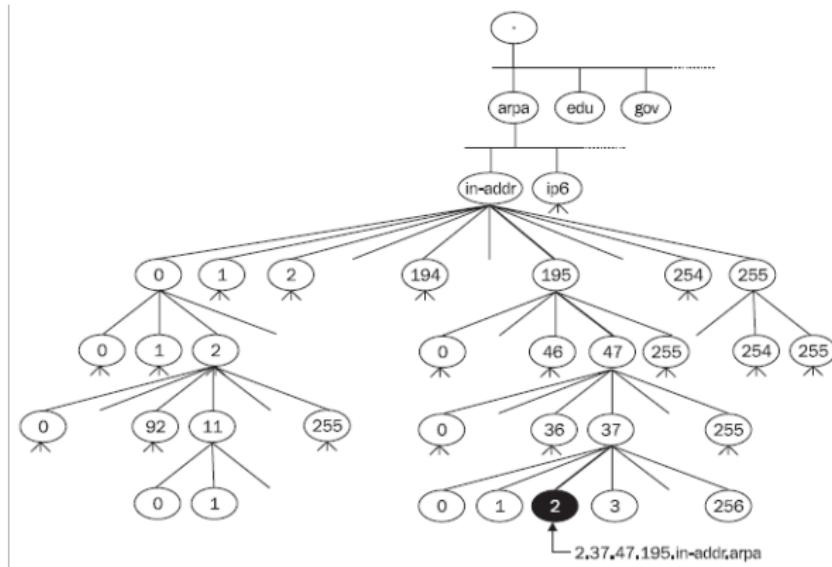
;; ADDITIONAL SECTION:
google.com.s9a2.psmtp.com. 14400 IN      A       74.125.148.11
google.com.s9b1.psmtp.com. 14400 IN      A       74.125.148.13
google.com.s9b2.psmtp.com. 14400 IN      A       74.125.148.14
google.com.s9a1.psmtp.com. 14400 IN      A       74.125.148.10

;; Query time: 313 msec
;; SERVER: 10.141.1.10#53(10.141.1.10)
;; WHEN: Sun Nov 15 21:24:39 2009
;; MSG SIZE  rcvd: 226
```

# Interroger les DNSs

Accéder aux contenus des enregistrements DNS : Résolution vs Résolution inverse

- ▶ Pour accélérer la résolution inverse, un autre domaine `arpa` (avec des sous domaines `in-addr` pour les adresses IPv4, `ip6` pour les IPv6, etc. ) ayant une structure d'arbre a été créé
- ▶ Les réponses se trouvent dans les enregistrements de type PTR



source : [www.codeguru.com](http://www.codeguru.com)

# Interroger les DNSs

Accéder aux contenus des enregistrements DNS : exemple avec nslookup

- *Forward lookup :*

nslookup hostname

Exemple : nslookup www.apache.org

- *Reverse lookup :*

nslookup IPadress

Exemple : nslookup 63.251.56.142

- "forward-lookup" et "reverse-lookup" n'accèdent pas nécessairement au même fichier pour trouver la réponse

- Parfois, il est utile de faire un "reverse-lookup" même si on connaît le nom de la machine. Il est possible que la requête retourne d'autres noms attribués à la machine qui aident à mieux comprendre son rôle.

# Interroger les DNSs

Accéder aux contenus des enregistrements DNS : exemple avec nslookup

- ➔ Quand le serveur est mal configuré, il est possible de faire un "zone-transfert" (transférer tous les enregistrements liés à un domaine ou une machine)
- ➔ Normalement, les "zone-transfert" doivent être permis seulement pour le serveur DNS secondaire afin qu'il puisse créer une copie identique au serveur primaire
- ➔ Le "zone-transfert" est généralement interdit par le serveur et même **illégal** dans certains endroits
- ➔ En effet, il donne trop d'informations : les enregistrement HINFO, par exemple, donnent même le systèmes d'exploitation et le type de cpu de la machine en question.

# Interroger les DNSs

Accéder aux contenus des enregistrements DNS : exemple avec nslookup  
Quand cela est possible, la séquence suivante permet de faire un "zone-transfert."

- Ouvrir une fenêtre de commande DOS
- Taper nslookup puis ENTER
- Taper set type=any puis ENTER : spécifie qu'on récupère tout
- ls -d target.com [> zone\_out.txt] puis ENTER : récupère les enregistrements (mettre le résultat dans le fichier zone\_out.txt comme option)
- exit puis ENTER : quitter nslookup

# Interroger les DNSs

Accéder aux contenus des enregistrements DNS : exemple avec nslookup

Le fichier dans lequel le résultat a été mis peut être traité par d'autres outils (grep, sed, awk, perl) pour accélérer l'analyse

- [bash]\$ grep -I solaris zone\_out | wc -l  
12
- Cela montre qu'il y a 12 machines de type solaris que l'intrus peut cibler

Zone transfert avec l'outil fierce : si le zone transfert n'est pas permis, fierce va « brutforcer » le serveur DNS par un ensemble de sous-domaines

```
root@kali:~# fierce -dns thesecurityblogger.com
DNS Servers for thesecurityblogger.com:
ns3.dreamhost.com
ns1.dreamhost.com
ns2.dreamhost.com

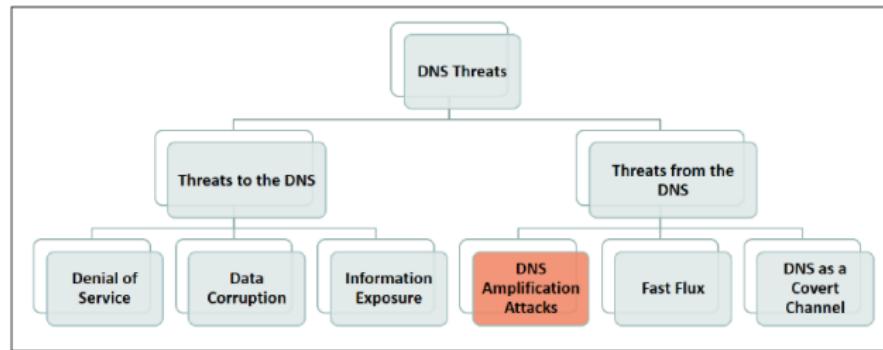
Trying zone transfer first...
Testing ns3.dreamhost.com
Request timed out or transfer not allowed.
Testing ns1.dreamhost.com
Request timed out or transfer not allowed.
Testing ns2.dreamhost.com
Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force
Can't open hosts.txt or the-default-wordlist
Exiting...
root@kali:~#
```

source : web penetration testing with kali linux

# Interroger les DNSs

## Menaces liées à DNS

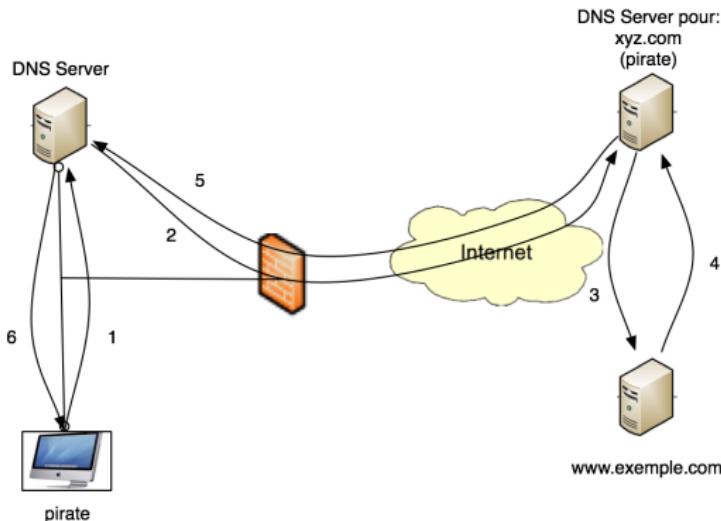


- DDOS : inonder une destination par un trafic
- Corruption de données : empoisonnement des caches DNS, répondre à une requête DNS avant le vrai serveur, prendre le contrôle d'un domaine (attaquer le compte du propriétaire dans un registraire), enregistrer des domaines très proches d'autres très connus et attendre les erreurs des utilisateurs.
- Le DNS contient des informations sensibles sur des machines et sur le réseau. Les réponses aux requêtes DNS circulent sans chiffrement
- Amplification du trafic (réponse plus volumineuse que la question) : requête de type TXT, ANY, etc. On peut passer de 60 octets à 4096 octets
- Fast-Flux : Changer rapidement l'adresse d'un serveur DNS
- DNS cover channel : envoyer les données d'un protocole quelconque à l'intérieur des requêtes/réponses DNS pour mieux traverser les pare-feux

# Interroger les DNSs

## HTTP dans DNS

- envoyer http dans DNS pour détourner un pare-feu



- ```

1- @IP of test1.example.com ?: get / http/ www.exemple.com
2- @IP of test1.example.com : get / http/ www.exemple.com
3- get / http/ www.exemple.com
4- http/ content ....
5- test1.example.com A 132.203.1.17 ::http /content ...
6- test1.example.com A 132.203.1.17 ::http /content ...
  
```

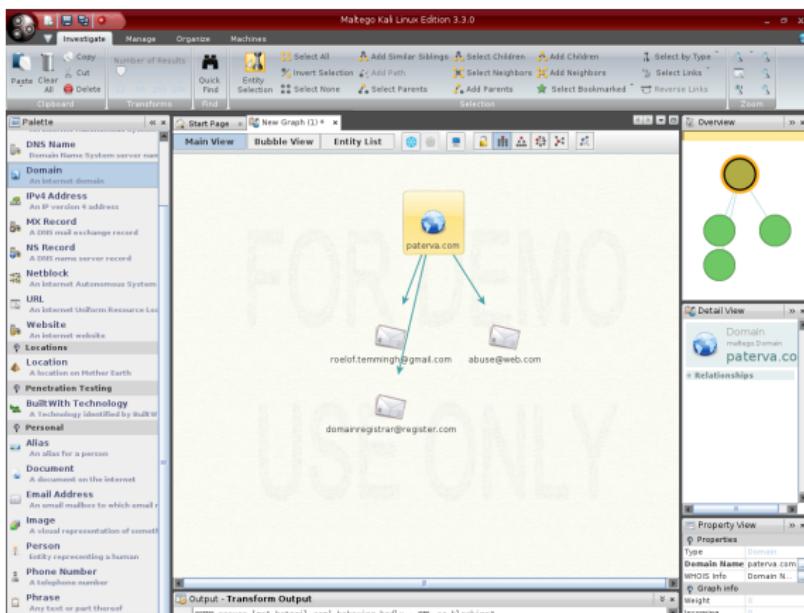
# Interroger les DNSs

## Contre mesures

- Configurer convenablement le serveur DNS
- Limiter le "zone-transfert" en utilisant la directive `allow-transfert` dans le fichier `named.conf` ou bien l'option `notify` pour les serveurs DNS Windows
- Interdire, via les pare-feux, toutes les connections non autorisées utilisant le protocole TCP et le port 53 (DNS). À noter qu'on utilise généralement UDP. Mais parfois on fait appel à TCP pour les requêtes ayant des réponses volumineuses telles que "zone-transfert"
- Limiter l'utilisation des enregistrements de type HINFO

# Outils de footprinting : Maltego

- Un couteau suisse pour le footprinting : noms de domaines, adresses courriels, noms de personnes, sites web, numéro de personnes, compte facebook, etc.
- Il est dans les top 10 des outils de Kali
- À ne pas manquer



# Outils de footprinting : HTTrack

- ➔ Outil d'aspiration de sites web
- ➔ Générer une copie (pages, images, liens, code, etc.) locale consultable hors connexion de la cible
- ➔ C'est gratuit (disponible sur <http://www.httack.co>) et il y a même une version avec interface graphique
- ➔ Pour l'installer sous Kali, la commande est : `apt-get install httrack`
- ➔ Pour le lancer, ouvrir un terminal et taper : `httrack`
- ➔ **Attention :** le clonage d'un site web est offensive et facile à repérer
- ➔ Une fois le site cloner, chercher les adresses physiques, les numéros de téléphone, les adresses courriel, les horaires d'ouvertures, les noms de partenaires, les noms des employés, les connexions médias sociaux, les actualités, les annonces, les offres d'emploi, les nouvelles économiques, les acquisitions, les technologies mises en oeuvre (matériel et logiciel), etc.

# Outils de footprinting : Google

Retenir la syntaxe de Google vous fait gagner beaucoup du temps durant la recherche

- *site* : cible.com
- *cache* : cible.com
- *allintitle* : index.of
- *inurl* : admin
- *inurl* : login logon Signin Signon Forgotpassword Forgot Reset
- *filetype* : pdf
- Une longue liste de hacking Google se trouve dans [www.exploit-db.com](http://www.exploit-db.com) (voir bouton GHDB : Google Hacking Database)

**Remarque :** N'oublier pas d'exploiter les autres moteurs de recherche (Yahoo, Bing, Ask, Dogpile, etc.), ils peuvent vous donner des meilleurs résultats que Google dans certains cas.

# Outils de footprinting : The Harvester

- Permet de rapidement cataloguer des adresses courriel, des sous domaines et des adresses IP directement liés à la cible
- Un script en Python intégré à Kali. Pour le lancer, ouvrir un terminal puis taper : *theharvester*
- Il cherche l'information dans le serveur de Google, Bing, PGP, Linkedin et autres
- Exemple d'utilisation :  
`theharvester -d cible.com -l 10 -b google`
- Les options -d (spécifie la cible) ; -l (limiter le nombre de sorties) -b (base de données de recherche : google, bing, pgp, linkedin, etc.)

# Autres Outils

- ➔ **whois** : trouver l'adresse physique, des courriels, des noms de contacts, des noms de serveurs dns et leurs adresses IP, l'intervalle d'adresse IP de la cible, etc. Syntaxe : *whois nom-cible*
- ➔ **www.whois.net** : le whois via le navigateur
- ➔ **netcraft** ([www.netcraft.com](http://www.netcraft.com)) : une excellente source d'information sur les sous domaines, les serveurs web de la cible, etc.
- ➔ **dig, nslookup, host** : interroger des serveurs DNS
- ➔ **ThreatAgent** : il utilise des techniques et des technologies variées pour créer un dossier complet sur la cible. il faut commencer par créer un compte gratuit sur [www.threatagent.com](http://www.threatagent.com)
- ➔ **www.iplocation.net** : géolocalisation via une adresse IP
- ➔ **Etc.**