

# **Footprinting e Ingeniería Social**

# Definición de Footprinting

- Footprinting es el proceso de creación de un mapa de las redes y sistemas de una organización.
- Está incluido en el proceso de “recopilación de información” (Information Gathering).
- El Footprinting comienza por la determinación del target, para luego averiguar información específica utilizando métodos no intrusivos.
- Una herramienta fundamental son las búsquedas online, utilizando Google u otro buscador. Es importante conocer en profundidad las características avanzadas de búsqueda (site:, intitle:, allinurl:, etc.)

# Definición de Footprinting (Cont.)

- Junto al escaneo y enumeración, el footprinting es una de las tres fases de obtención de información antes de un ataque.
- Un atacante suele utilizar el 90% de su tiempo en las primeras etapas.
- El footprinting resultará en un único perfil en la red para cada organización.

# Metodología de Recopilación de Información

- La obtención de información sobre un objetivo se realiza antes de un ataque.
- La metodología utilizada considera tres etapas: *Footprinting*, *Scanning* y *Enumeration*.
- De manera general puede ser dividida en siete pasos.
  - Detectar la información inicial
  - Ubicación del rango de red
  - Comprobación de equipos activos
  - Descubrimiento de puertos abiertos y puntos de acceso
  - Detección del sistema operativo
  - Descubrimiento de servicios en los puertos
  - Mapeo de red
- El proceso de footprinting se realiza durante los primeros dos pasos.

# Metodología de Recopilación de Información (Cont.)

- Algunas fuentes comunes de información incluyen el uso de:
  - Domain name lookup
  - Whois
  - Nslookup
- La mayor parte de la información puede obtenerse libremente y de manera legal.
- Es muy importante comprender el sistema de resolución de nombres de dominio (DNS) para lograr una profunda comprensión de esta etapa y del funcionamiento de Internet.

# Búsqueda de Información en Internet

- Buscando en Internet la dirección de correo electrónico o el nombre de una persona podemos encontrar en las listas de correo, foros, etc. información sobre la empresa donde trabaja.
- Otra fuente de información útil son las redes sociales y los sitios de empleos.

- Esta iniciativa guarda la mayor parte de los sitios web de Internet y alberga obras culturales de dominio público o con licencias abiertas.
- Se dedica desde 1996 a recoger sistemáticamente copias de los sitios web de todo el mundo, permitiendo estudiar su evolución.
- La herramienta que permite consultar sitios históricos se denomina: *Wayback Machine*

# Archivo Histórico: <http://www.archive.org> (Cont.)



Enter Web Address:

All

Take Me Back

[Adv. Search](#) [Compare Archive Pages](#)

Searched for <http://www.google.com>

3612 Results

Note some duplicates are not shown. [See all.](#)

\* denotes when site was updated.

Material typically becomes available here 6 months after collection. [See FAQ.](#)

## Search Results for Jan 01, 1996 - Mar 20, 2008

| 1996    | 1997    | 1998                           | 1999                           | 2000                           | 2001                           | 2002                           | 2003                           | 2004                           | 2005                           | 2006                           | 2007                           | 2008                           |
|---------|---------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|
| 0 pages | 0 pages | 2 pages                        | 12 pages                       | 73 pages                       | 685 pages                      | 154 pages                      | 61 pages                       | 205 pages                      | 910 pages                      | 348 pages                      | 458 pages                      | 21 pages                       |
|         |         | <a href="#">Nov 11, 1998</a> * | <a href="#">Jan 17, 1999</a> * | <a href="#">Feb 29, 2000</a> * | <a href="#">Jan 18, 2001</a> * | <a href="#">Jan 23, 2002</a> * | <a href="#">Feb 02, 2003</a> * | <a href="#">Jan 03, 2004</a> * | <a href="#">Jan 01, 2005</a>   | <a href="#">Jan 01, 2006</a> * | <a href="#">Jan 01, 2007</a> * | <a href="#">Jan 02, 2008</a> * |
|         |         | <a href="#">Dec 02, 1998</a> * | <a href="#">Jan 25, 1999</a> * | <a href="#">Mar 01, 2000</a> * | <a href="#">Jan 19, 2001</a> * | <a href="#">Jan 24, 2002</a> * | <a href="#">Feb 04, 2003</a> * | <a href="#">Jan 13, 2004</a> * | <a href="#">Jan 01, 2005</a> * | <a href="#">Jan 01, 2006</a> * | <a href="#">Jan 01, 2007</a> * | <a href="#">Jan 02, 2008</a> * |
|         |         |                                | <a href="#">Feb 08, 1999</a> * | <a href="#">Mar 01, 2000</a> * | <a href="#">Jan 19, 2001</a> * | <a href="#">Jan 24, 2002</a> * | <a href="#">Feb 05, 2003</a> * | <a href="#">Jan 21, 2004</a>   | <a href="#">Jan 02, 2005</a>   | <a href="#">Jan 01, 2006</a> * | <a href="#">Jan 02, 2007</a> * | <a href="#">Jan 14, 2008</a> * |
|         |         |                                | <a href="#">Apr 22, 1999</a> * | <a href="#">Mar 02, 2000</a>   | <a href="#">Jan 19, 2001</a> * | <a href="#">Feb 06, 2002</a> * | <a href="#">Feb 08, 2003</a>   | <a href="#">Jan 26, 2004</a>   | <a href="#">Jan 02, 2005</a> * | <a href="#">Jan 02, 2006</a> * | <a href="#">Jan 02, 2007</a> * | <a href="#">Jan 16, 2008</a> * |
|         |         |                                | <a href="#">Apr 23, 1999</a>   | <a href="#">Mar 03, 2000</a>   | <a href="#">Jan 19, 2001</a> * | <a href="#">Feb 22, 2002</a> * | <a href="#">Feb 14, 2003</a> * | <a href="#">Jan 29, 2004</a>   | <a href="#">Jan 03, 2005</a>   | <a href="#">Jan 02, 2006</a> * | <a href="#">Jan 03, 2007</a> * | <a href="#">Jan 19, 2008</a> * |
|         |         |                                | <a href="#">Apr 27, 1999</a>   | <a href="#">Mar 04, 2000</a>   | <a href="#">Jan 19, 2001</a> * | <a href="#">Feb 23, 2002</a>   | <a href="#">Feb 15, 2003</a>   | <a href="#">Feb 08, 2004</a> * | <a href="#">Jan 05, 2005</a> * | <a href="#">Jan 03, 2006</a>   | <a href="#">Jan 03, 2007</a> * | <a href="#">Jan 22, 2008</a> * |
|         |         |                                | <a href="#">Apr 28, 1999</a>   | <a href="#">Apr 07, 2000</a> * | <a href="#">Jan 19, 2001</a> * | <a href="#">Mar 31, 2002</a> * | <a href="#">Feb 17, 2003</a> * | <a href="#">Feb 11, 2004</a>   | <a href="#">Jan 06, 2005</a> * | <a href="#">Jan 03, 2006</a> * | <a href="#">Jan 04, 2007</a> * | <a href="#">Jan 28, 2008</a> * |
|         |         |                                | <a href="#">May 08, 1999</a>   | <a href="#">Apr 08, 2000</a>   | <a href="#">Jan 19, 2001</a> * | <a href="#">Apr 02, 2002</a>   | <a href="#">Feb 17, 2003</a> * | <a href="#">Feb 15, 2004</a> * | <a href="#">Jan 06, 2005</a> * | <a href="#">Jan 03, 2006</a> * | <a href="#">Jan 04, 2007</a> * | <a href="#">Feb 07, 2008</a> * |
|         |         |                                | <a href="#">Oct 01, 1999</a> * | <a href="#">Apr 09, 2000</a>   | <a href="#">Jan 19, 2001</a> * | <a href="#">May 23, 2002</a> * | <a href="#">Mar 24, 2003</a> * | <a href="#">Feb 18, 2004</a> * | <a href="#">Jan 07, 2005</a> * | <a href="#">Jan 03, 2006</a> * | <a href="#">Jan 05, 2007</a> * | <a href="#">Feb 08, 2008</a> * |
|         |         |                                | <a href="#">Oct 12, 1999</a>   | <a href="#">May 10, 2000</a> * | <a href="#">Feb 01, 2001</a>   | <a href="#">May 25, 2002</a> * | <a href="#">Mar 28, 2003</a> * | <a href="#">Feb 25, 2004</a> * | <a href="#">Jan 07, 2005</a> * | <a href="#">Jan 03, 2006</a> * | <a href="#">Jan 05, 2007</a> * | <a href="#">Feb 09, 2008</a> * |
|         |         |                                | <a href="#">Nov 06, 1999</a> * | <a href="#">May 10, 2000</a> * | <a href="#">Feb 24, 2001</a>   | <a href="#">Jun 02, 2002</a>   | <a href="#">Mar 29, 2003</a>   | <a href="#">Feb 27, 2004</a> * | <a href="#">Jan 07, 2005</a> * | <a href="#">Jan 04, 2006</a>   | <a href="#">Jan 06, 2007</a>   | <a href="#">Feb 11, 2008</a> * |
|         |         |                                | <a href="#">Nov 29, 1999</a> * | <a href="#">May 10, 2000</a> * | <a href="#">Feb 26, 2001</a> * | <a href="#">Jun 04, 2002</a> * | <a href="#">Apr 02, 2003</a>   | <a href="#">Mar 06, 2004</a>   | <a href="#">Jan 08, 2005</a> * | <a href="#">Jan 04, 2006</a> * | <a href="#">Jan 06, 2007</a> * | <a href="#">Feb 13, 2008</a> * |
|         |         |                                |                                | <a href="#">May 10, 2000</a> * | <a href="#">Mar 01, 2001</a>   | <a href="#">Jun 05, 2002</a>   | <a href="#">Apr 03, 2003</a> * | <a href="#">Mar 25, 2004</a> * | <a href="#">Jan 09, 2005</a>   | <a href="#">Jan 04, 2006</a> * | <a href="#">Jan 06, 2007</a> * | <a href="#">Feb 15, 2008</a> * |
|         |         |                                |                                | <a href="#">May 10, 2000</a> * | <a href="#">Mar 01, 2001</a> * | <a href="#">Jul 02, 2002</a> * | <a href="#">Apr 09, 2003</a>   | <a href="#">Mar 31, 2004</a> * | <a href="#">Jan 09, 2005</a> * | <a href="#">Jan 05, 2006</a> * | <a href="#">Jan 07, 2007</a> * | <a href="#">Feb 16, 2008</a> * |
|         |         |                                |                                | <a href="#">May 10, 2000</a> * | <a href="#">Mar 01, 2001</a> * | <a href="#">Jul 03, 2002</a> * | <a href="#">Apr 21, 2003</a> * | <a href="#">Apr 01, 2004</a>   | <a href="#">Jan 11, 2005</a> * | <a href="#">Jan 05, 2006</a> * | <a href="#">Jan 07, 2007</a> * | <a href="#">Feb 22, 2008</a> * |
|         |         |                                |                                | <a href="#">May 11, 2000</a>   | <a href="#">Mar 01, 2001</a> * | <a href="#">Jul 04, 2002</a> * | <a href="#">Apr 23, 2003</a>   | <a href="#">Apr 03, 2004</a>   | <a href="#">Jan 14, 2005</a>   | <a href="#">Jan 05, 2006</a> * | <a href="#">Jan 08, 2007</a> * | <a href="#">Feb 27, 2008</a> * |
|         |         |                                |                                | <a href="#">May 11, 2000</a> * | <a href="#">Mar 02, 2001</a>   | <a href="#">Jul 07, 2002</a> * | <a href="#">Apr 28, 2003</a>   | <a href="#">Apr 03, 2004</a> * | <a href="#">Jan 15, 2005</a>   | <a href="#">Jan 06, 2006</a> * | <a href="#">Jan 08, 2007</a> * | <a href="#">Mar 06, 2008</a> * |
|         |         |                                |                                | <a href="#">May 11, 2000</a> * | <a href="#">Mar 31, 2001</a> * | <a href="#">Jul 09, 2002</a> * | <a href="#">May 01, 2003</a>   | <a href="#">Apr 04, 2004</a>   | <a href="#">Jan 15, 2005</a> * | <a href="#">Jan 06, 2006</a> * | <a href="#">Jan 08, 2007</a> * | <a href="#">Mar 07, 2008</a> * |
|         |         |                                |                                | <a href="#">May 11, 2000</a> * | <a href="#">Mar 31, 2001</a> * | <a href="#">Jul 20, 2002</a> * | <a href="#">May 12, 2003</a>   | <a href="#">Apr 07, 2004</a>   | <a href="#">Jan 15, 2005</a> * | <a href="#">Jan 10, 2006</a> * | <a href="#">Jan 08, 2007</a> * | <a href="#">Mar 08, 2008</a> * |
|         |         |                                |                                | <a href="#">May 11, 2000</a> * | <a href="#">Apr 01, 2001</a>   | <a href="#">Jul 26, 2002</a>   | <a href="#">May 27, 2003</a>   | <a href="#">Apr 26, 2004</a> * | <a href="#">Jan 16, 2005</a>   | <a href="#">Jan 10, 2006</a> * | <a href="#">Jan 09, 2007</a> * | <a href="#">Mar 15, 2008</a> * |
|         |         |                                |                                | <a href="#">May 11, 2000</a> * | <a href="#">Apr 02, 2001</a> * | <a href="#">Aug 02, 2002</a> * | <a href="#">May 30, 2003</a>   | <a href="#">Apr 28, 2004</a> * | <a href="#">Jan 17, 2005</a> * | <a href="#">Jan 10, 2006</a> * | <a href="#">Jan 09, 2007</a> * | <a href="#">Mar 18, 2008</a> * |
|         |         |                                |                                | <a href="#">May 11, 2000</a> * | <a href="#">Apr 04, 2001</a> * | <a href="#">Aug 02, 2002</a> * | <a href="#">Jun 01, 2003</a>   | <a href="#">May 06, 2004</a> * | <a href="#">Jan 18, 2005</a> * | <a href="#">Jan 10, 2006</a> * | <a href="#">Jan 10, 2007</a> * |                                |
|         |         |                                |                                | <a href="#">May 12, 2000</a> * | <a href="#">Apr 04, 2001</a> * | <a href="#">Aug 03, 2002</a>   | <a href="#">Jun 02, 2003</a> * | <a href="#">May 12, 2004</a> * | <a href="#">Jan 19, 2005</a> * | <a href="#">Jan 10, 2006</a> * | <a href="#">Jan 11, 2007</a> * |                                |
|         |         |                                |                                | <a href="#">May 12, 2000</a> * | <a href="#">Apr 10, 2001</a>   | <a href="#">Aug 05, 2002</a>   | <a href="#">Jun 06, 2003</a> * | <a href="#">May 18, 2004</a> * | <a href="#">Jan 19, 2005</a> * | <a href="#">Jan 10, 2006</a> * | <a href="#">Jan 11, 2007</a> * |                                |
|         |         |                                |                                | <a href="#">May 12, 2000</a> * | <a href="#">Apr 13, 2001</a> * | <a href="#">Aug 06, 2002</a> * | <a href="#">Jun 13, 2003</a> * | <a href="#">May 20, 2004</a> * | <a href="#">Jan 20, 2005</a> * | <a href="#">Jan 10, 2006</a> * | <a href="#">Jan 11, 2007</a> * |                                |
|         |         |                                |                                | <a href="#">May 12, 2000</a> * | <a href="#">Apr 30, 2001</a> * | <a href="#">Aug 07, 2002</a> * | <a href="#">Jun 22, 2003</a>   | <a href="#">May 25, 2004</a> * | <a href="#">Jan 20, 2005</a> * | <a href="#">Jan 11, 2006</a> * | <a href="#">Jan 12, 2007</a> * |                                |
|         |         |                                |                                | <a href="#">May 19, 2000</a> * | <a href="#">May 03, 2001</a>   | <a href="#">Aug 08, 2002</a> * | <a href="#">Jun 23, 2003</a>   | <a href="#">May 27, 2004</a>   | <a href="#">Jan 21, 2005</a>   | <a href="#">Jan 11, 2006</a> * | <a href="#">Jan 12, 2007</a> * |                                |
|         |         |                                |                                | <a href="#">May 20, 2000</a> * | <a href="#">May 04, 2001</a>   | <a href="#">Aug 08, 2002</a> * | <a href="#">Jun 24, 2003</a> * | <a href="#">Jun 06, 2004</a> * | <a href="#">Jan 23, 2005</a>   | <a href="#">Jan 11, 2006</a> * | <a href="#">Jan 13, 2007</a>   |                                |
|         |         |                                |                                | <a href="#">Jun 19, 2000</a>   | <a href="#">May 04, 2001</a> * | <a href="#">Aug 09, 2002</a>   | <a href="#">Jun 30, 2003</a> * | <a href="#">Jun 06, 2004</a> * | <a href="#">Jan 24, 2005</a>   | <a href="#">Jan 11, 2006</a> * | <a href="#">Jan 13, 2007</a> * |                                |
|         |         |                                |                                | <a href="#">Jun 19, 2000</a> * | <a href="#">May 05, 2001</a> * | <a href="#">Aug 10, 2002</a> * | <a href="#">Jul 21, 2003</a>   | <a href="#">Jun 08, 2004</a>   | <a href="#">Jan 24, 2005</a> * | <a href="#">Jan 11, 2006</a> * | <a href="#">Jan 14, 2007</a>   |                                |
|         |         |                                |                                | <a href="#">Jun 20, 2000</a>   | <a href="#">May 05, 2001</a> * | <a href="#">Aug 11, 2002</a>   | <a href="#">Aug 01, 2003</a>   | <a href="#">Jun 08, 2004</a> * | <a href="#">Jan 25, 2005</a> * | <a href="#">Jan 12, 2006</a> * | <a href="#">Jan 14, 2007</a> * |                                |
|         |         |                                |                                | <a href="#">Jun 21, 2000</a>   | <a href="#">May 06, 2001</a>   | <a href="#">Aug 12, 2002</a> * | <a href="#">Aug 02, 2003</a> * | <a href="#">Jun 09, 2004</a> * | <a href="#">Jan 26, 2005</a> * | <a href="#">Jan 12, 2006</a> * | <a href="#">Jan 15, 2007</a> * |                                |
|         |         |                                |                                | <a href="#">Jun 21, 2000</a> * | <a href="#">May 06, 2001</a> * | <a href="#">Aug 12, 2002</a> * | <a href="#">Aug 04, 2003</a> * | <a href="#">Jun 11, 2004</a> * | <a href="#">Jan 27, 2005</a> * | <a href="#">Jan 12, 2006</a> * | <a href="#">Jan 15, 2007</a> * |                                |
|         |         |                                |                                | <a href="#">Jun 22, 2000</a>   | <a href="#">May 06, 2001</a> * | <a href="#">Aug 13, 2002</a> * | <a href="#">Aug 05, 2003</a>   | <a href="#">Jun 12, 2004</a>   | <a href="#">Jan 27, 2005</a> * | <a href="#">Jan 12, 2006</a> * | <a href="#">Jan 16, 2007</a> * |                                |
|         |         |                                |                                | <a href="#">Jun 22, 2000</a> * | <a href="#">May 06, 2001</a> * | <a href="#">Aug 13, 2002</a> * | <a href="#">Aug 07, 2003</a> * | <a href="#">Jun 14, 2004</a>   | <a href="#">Jan 30, 2005</a> * | <a href="#">Jan 12, 2006</a> * | <a href="#">Jan 16, 2007</a> * |                                |
|         |         |                                |                                | <a href="#">Jul 11, 2000</a> * | <a href="#">May 06, 2001</a> * | <a href="#">Aug 14, 2002</a> * | <a href="#">Sep 26, 2003</a> * | <a href="#">Jun 15, 2004</a>   | <a href="#">Jan 30, 2005</a> * | <a href="#">Jan 13, 2006</a>   | <a href="#">Jan 16, 2007</a> * |                                |



# DNS Zone Transfer

- Los datos contenidos en una zona DNS son sensibles por naturaleza.
- Individualmente, los registros DNS no son sensibles, pero si un atacante obtiene una copia entera de la zona DNS de un dominio, obtiene una lista completa de todos los Host de ese dominio.
- Un atacante no necesita herramientas especiales para obtener una zona DNS completa, solo que el DNS este mal configurado y que permita a cualquiera realizar una transferencia de zona.
- La transferencia de zona es necesaria y no pueden ser deshabilitadas completamente. Pero solo deben ser permitidas entre servidores DNS y clientes que necesitan de estas.
- En generalmente solo los servidores DNS dependientes necesitan realizar transferencia de zona.

# DNS Denial of Service

- Si un atacante puede realizar una transferencia de zona, también puede realizar ataques de denegación de servicio contra esos servidores DNS realizando múltiples peticiones.

# Identificación de los Tipos de Registros DNS

- **A (address):** Mapea un nombre de host a una dirección IP
- **SOA (Start of Authority):** Define el DNS responsable de la información del dominio.
- **CNAME (canonical name):** Provee nombres adicionales o alias para dicho registro.
- **MX (mail exchange):** Identifica el mailserver del dominio.
- **SRV (service):** Identifica servicios que ofrece el dominio.
- **PTR (pointer):** Mapea direcciones IP a nombres de host

# Identificación de los Tipos de Registros DNS (Cont.)

- **NS (name server):** Identifica otros servidores de nombres para el dominio.
- **HINFO:** Información del host, equipo y sistema operativo
- **TXT:** Información de texto. Permite a los dominios identificarse de modos arbitrarios
- **LOC:** Permite indicar las coordenadas del dominio.
- **WKS:** Generalización del registro MX para indicar los servicios que ofrece el dominio. Está obsoleto en favor de SRV.

# Whois y ARIN Lookups

- Whois es una herramienta y un protocolo que identifica información de registración de un dominio. Esta definido en el RFC 3912.
- El whois evolucionó desde los primeros Unix hasta los actuales. Las consultas se han realizado tradicionalmente usando una interfaz de línea de comandos, pero actualmente existen multitud de páginas web que permiten realizar estas consultas, aunque siguen dependiendo internamente del protocolo original.
- Utilizando whois, es posible recopilar información de registro como ser el nombre de la persona que realizó el registro del dominio, su correo electrónico, número telefónico y números IP de sus servidores principales.
- Esta información puede atentar contra la privacidad y permitir a los spammers capturar direcciones.

# Whois y ARIN Lookups (Cont.)

- Una URL (uniform resource locator) como `www.google.com` contiene un nombre de dominio (`google.com`) y un hostname o alias (`www`).
- La organización ICANN (Internet Corporation for Assigned Names and Numbers) requiere el registro de dominios para asegurar la unicidad de los mismos.
- Las herramientas de whois recogen información sobre este registro oficial y obligatorio.

# Herramienta: <http://www.dnsstuff.com/>

## -FREE DNS Tools-

**WHOIS/IPWHOIS Lookup** ?

WHOIS

Enter domain or host name or IP  
Advanced version available in [Professional Tool Set >](#)

**IP Information** ?

Shows info about an IP, including city and country

Lookup

Enter IP

**Traceroute** ?

Traces the route packets take to this host.

Traceroute

Enter host name (or IP)  
Advanced version available in [Professional Tool Set >](#)

**Country IP Range Lookup** ?

Lookup

Enter Country (eg 'cn' or 'china')

**CSE HTML Validator** ?

Finds HTML errors in websites.

Validate

Enter website URL

**Random Number Generator** ?

Get Number

Enter # of bits (1->1024)

**RFC Lookup** ?

Lookup

Enter RFC number (eg 821)

**URL DEOBFUSCATOR** ?

De-obfuscates confusing URLs.

Deobfuscate

Enter URL

**Country Tool** ?

Lookup

Enter country or TLD

**Punycode Converter** ?

Lookup

Enter Punycode or Unicode domain

**Wake-On-LAN** ?

Lookup

IP / MAC / Port

**Decimal IPs** ?

Converts a decimal IP (e.g. 2130706433) into an IP.

Decimal

Enter decimal IP

**RADB Routing** ?

Lookup

Enter IP

**Free E-mail Lookup** ?

Is an E-mail address a known free one?

Free Mail

Enter E-mail address or domain

**What does a website know about you?** ?

Find Out!

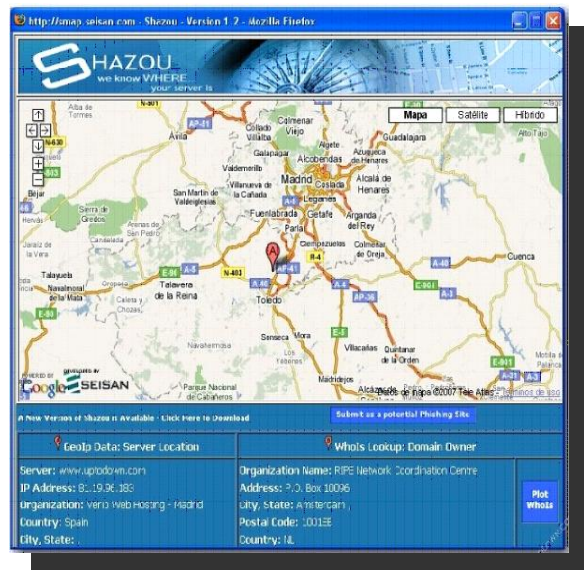
Displays information about your IP, OS, Browser, DNS

**Does your computer leak Netbios info?** ?

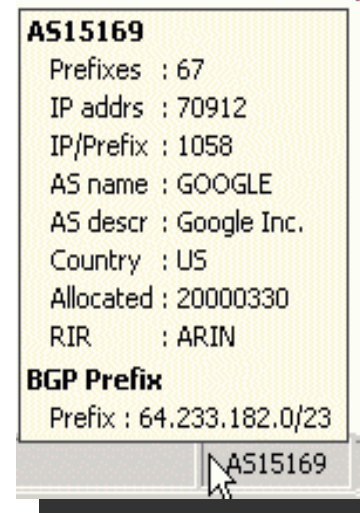
Find Out!

Displays information about Netbios on your computer

# Herramientas: Firefox Plugins



Shazou



AS Number



ShowIP

## Firefox Plugin: hostipfox

Download the new plugin now and tell us what you think.

Plugin: [hostipfox-0.2.1.xpi](#)

How it works: It plays IP Trace information when you hover over a li

## it this on You

Address: <http://www.hostip.info/firefox/hostipfox-0.2.1.x>

Host: www.hostip.info

IP: 66.102.124.100

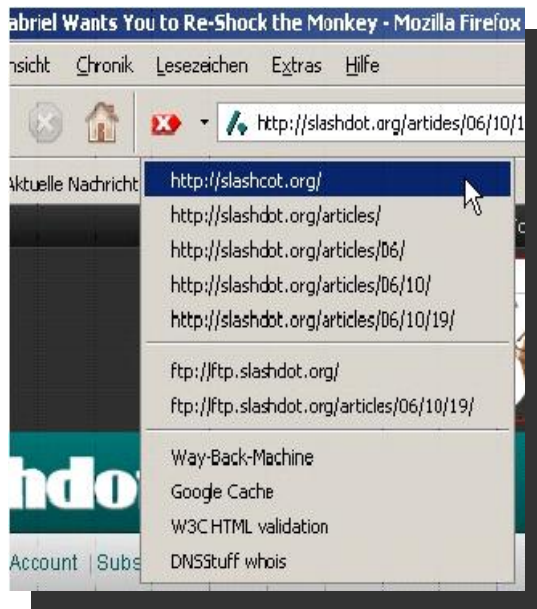
Location: Vancouver, CA

HOWTO put an IP Address Lookup using a **shell script**

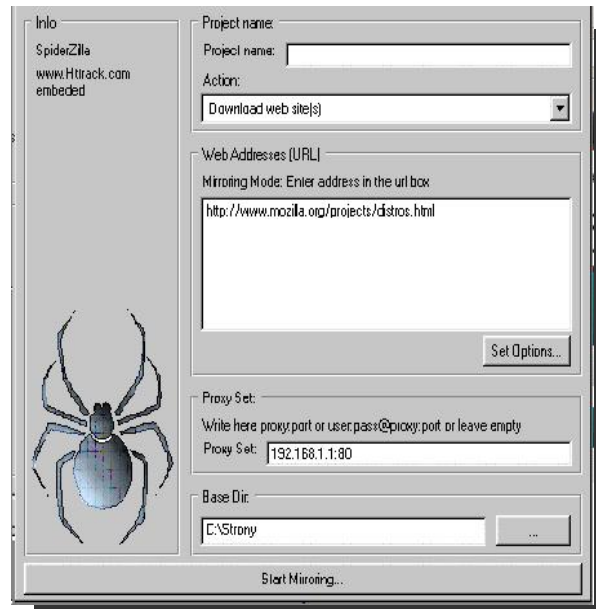
Hostipfox



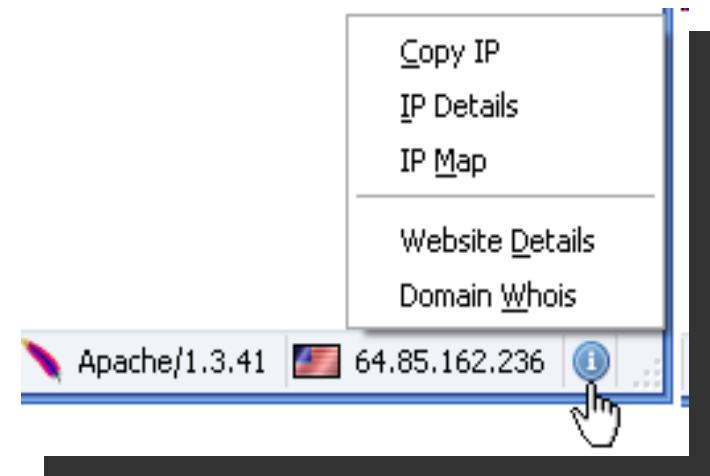
# Herramientas: Firefox Plugins



DiggiDig



SpiderZilla

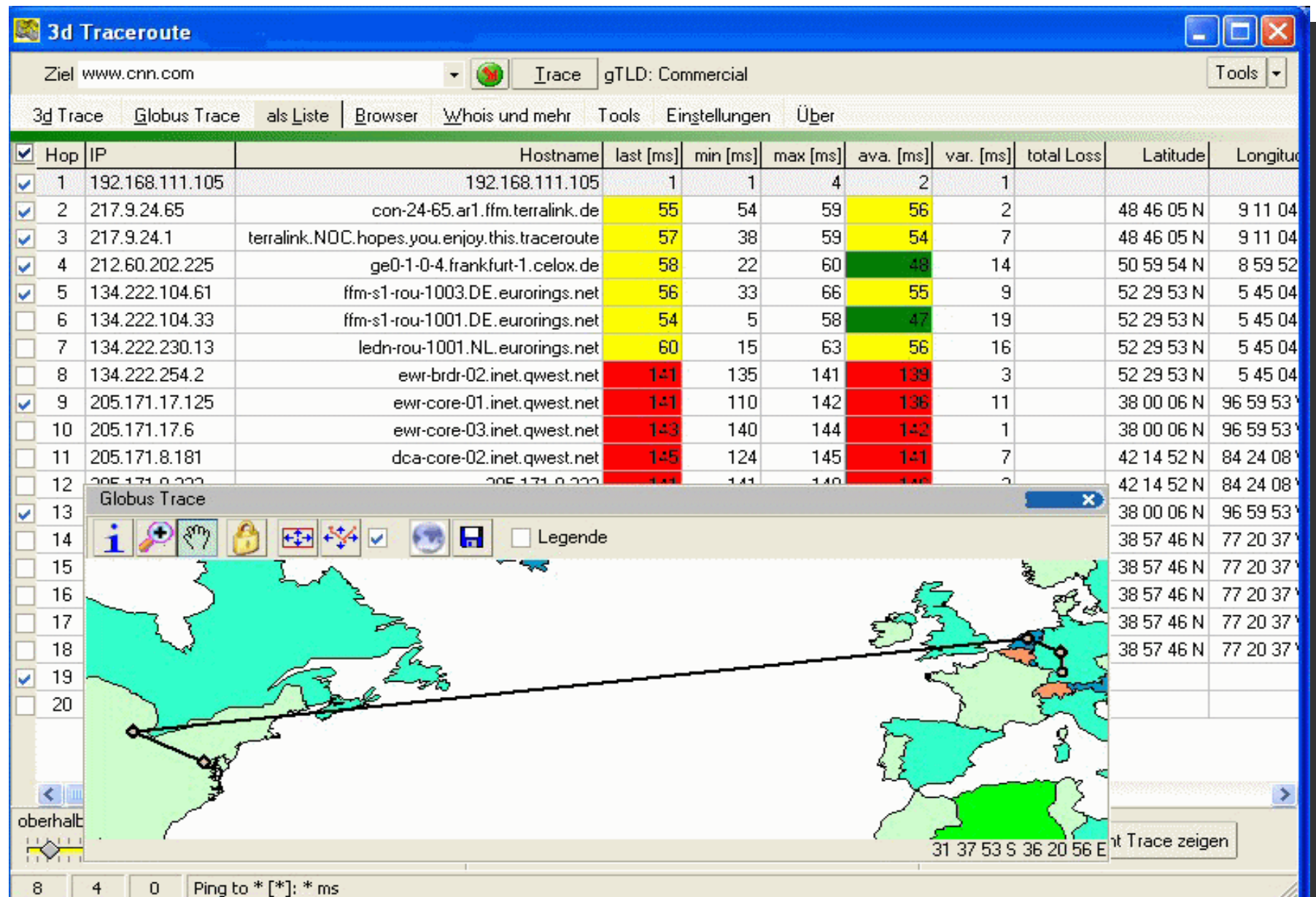


Domain Details

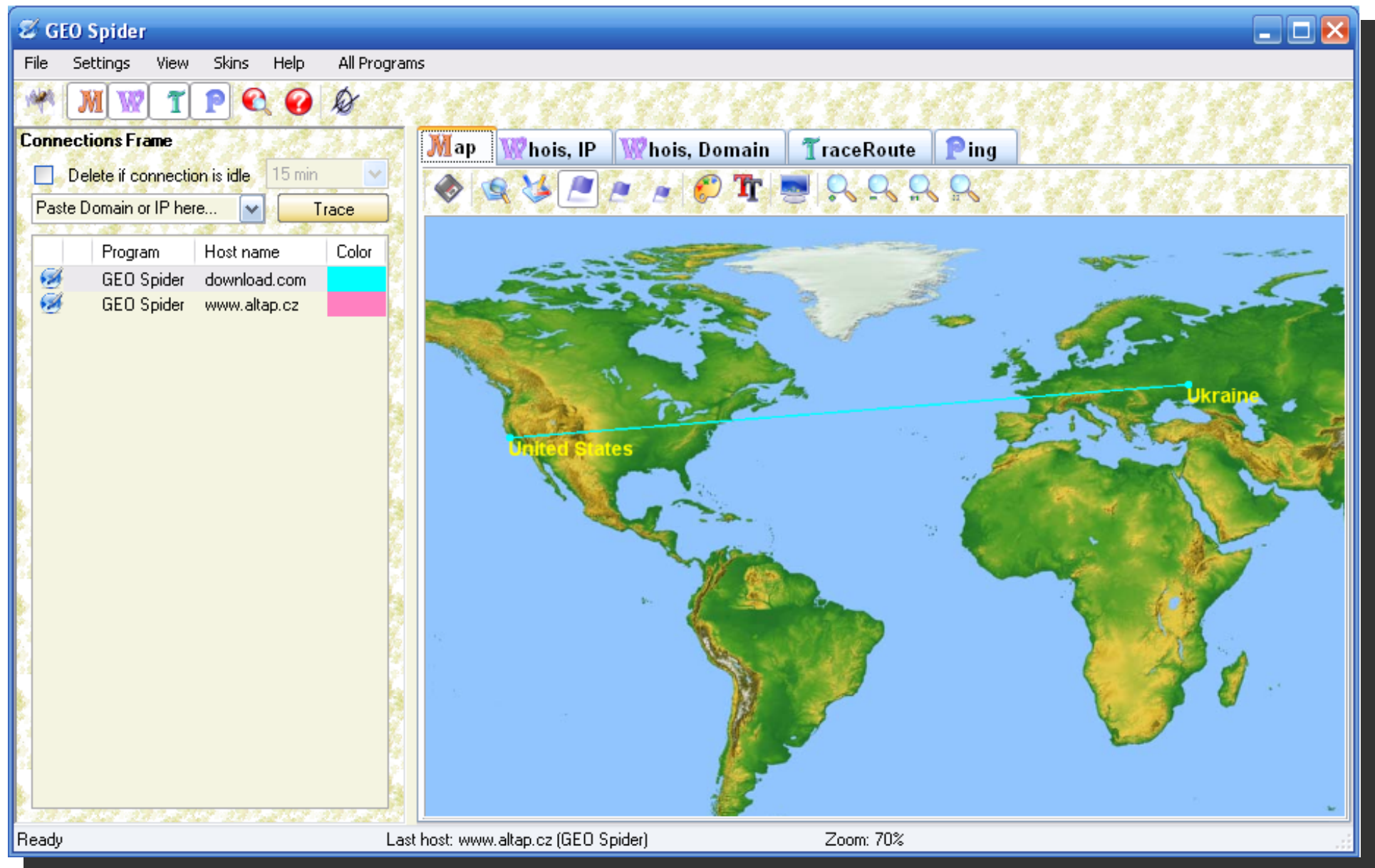
# Traceroute en el Footprinting

- *Traceroute* es una herramienta disponible en todos los S.O. que se utiliza para determinar la ruta de una conexión mediante el envío de un paquete ICMP echo a cada salto (router o gateway) a través del camino hasta el destino.
- Cuando los paquetes son devueltos del router, el TTL (time to live) se decrementa en un punto por cada router a lo largo de la ruta.
- Esto permite determinar cuántos saltos existen desde el origen hasta el destino.
- Uno de los problemas del uso del *traceroute* son los “times out” (indicados con un asterisco). Esto ocurre normalmente al encontrarse un firewall, lo cual también brinda información sobre su existencia y permite luego utilizar técnicas para saltarlo (bypass).
- Las herramientas de *traceroute* visuales pueden ayudar mucho a clarificar las rutas.

# Herramienta: 3D Traceroute



# Herramienta: GEO Spider

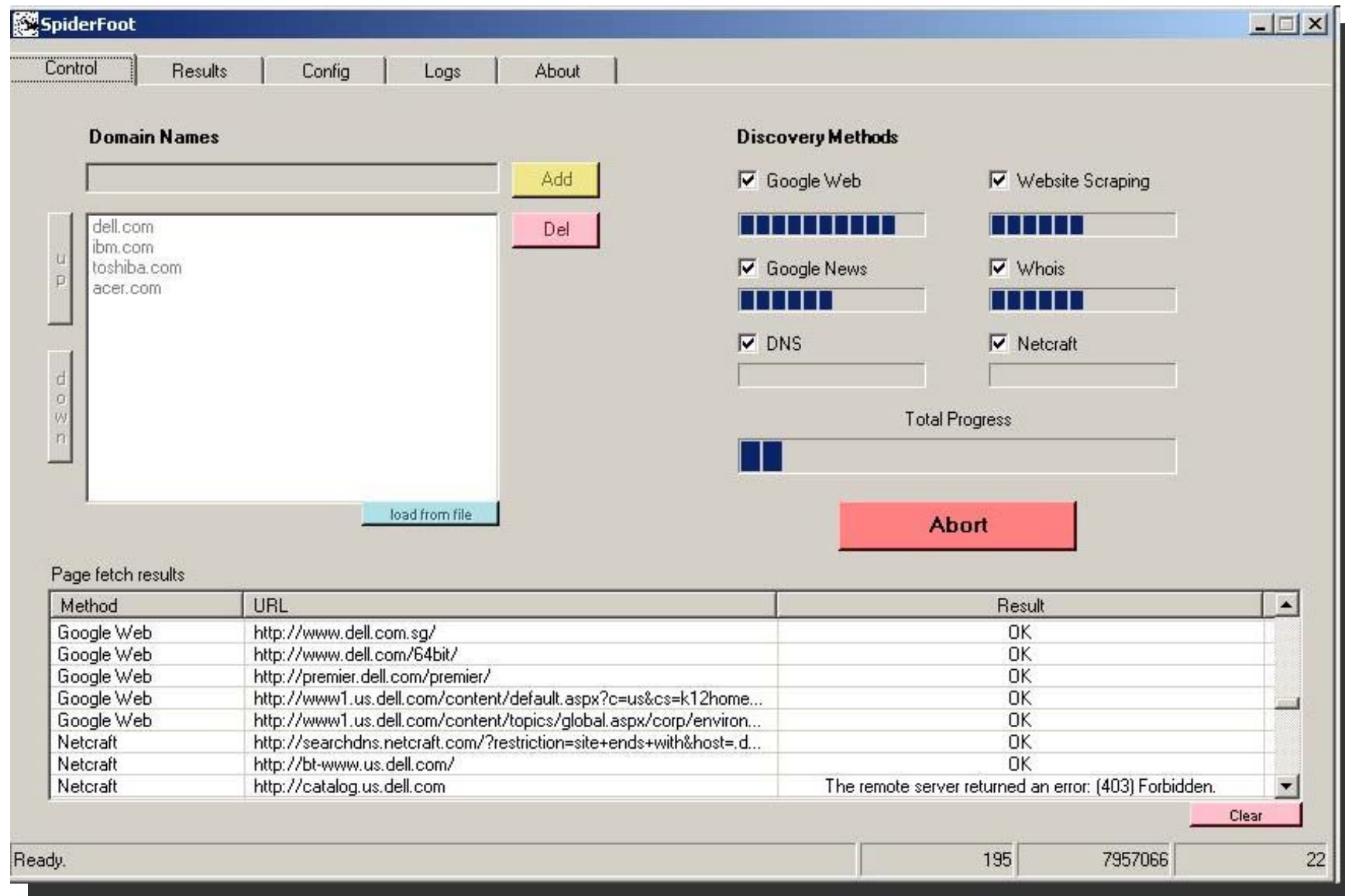


# Web Spiders

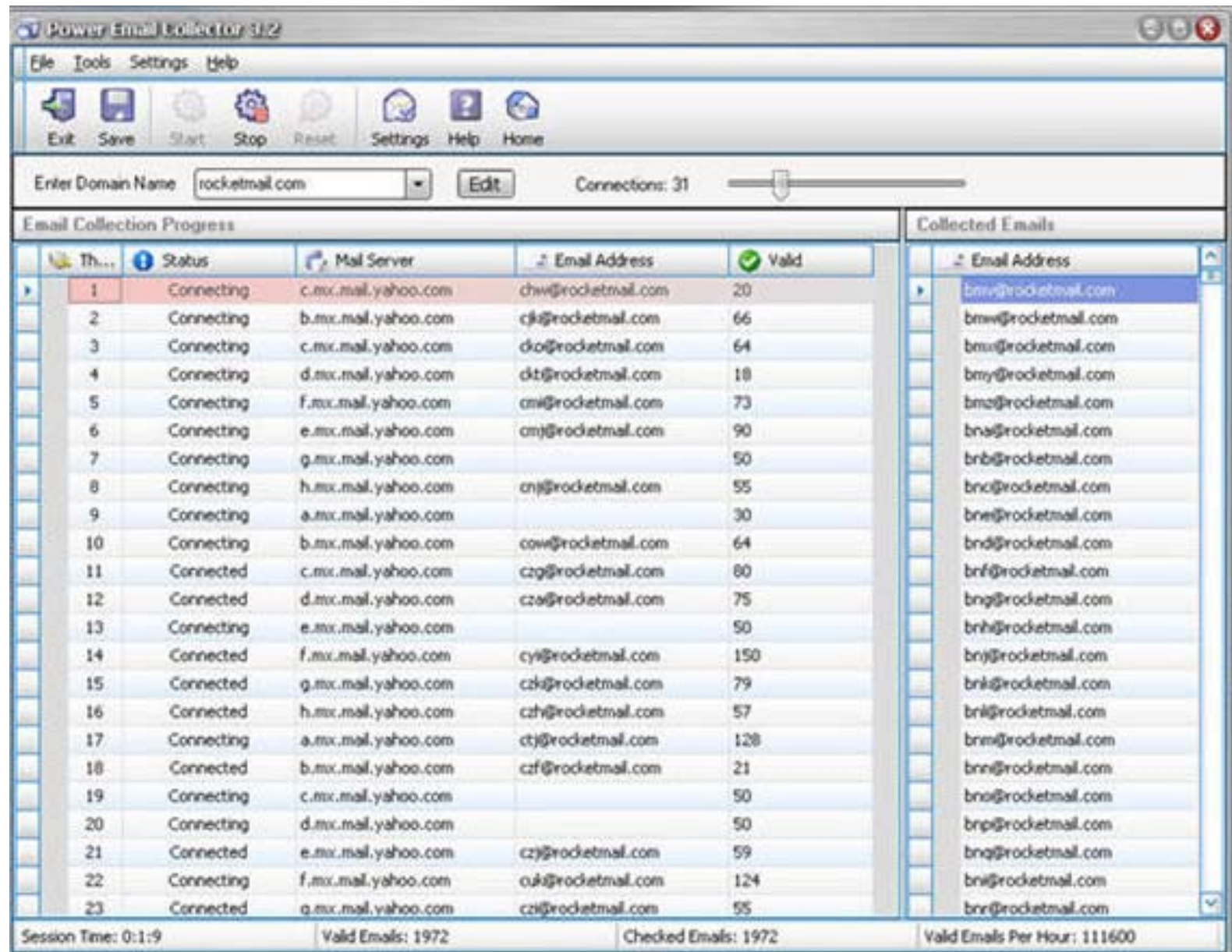
- Los spammers y todo interesado en recolectar direcciones de e-mail utilizan web spiders para encontrar direcciones.
- Los web spiders también pueden ser utilizados para encontrar otro tipo de información y pueden automatizar el proceso de reconocimiento.
- Un método para prevenirse del web *spidering* es el uso del archivo “robots.txt” en la raíz del sitio web, indicando la lista de directorios que desea protegerse de la averiguación. Notar que esto también brinda información adicional ;-)



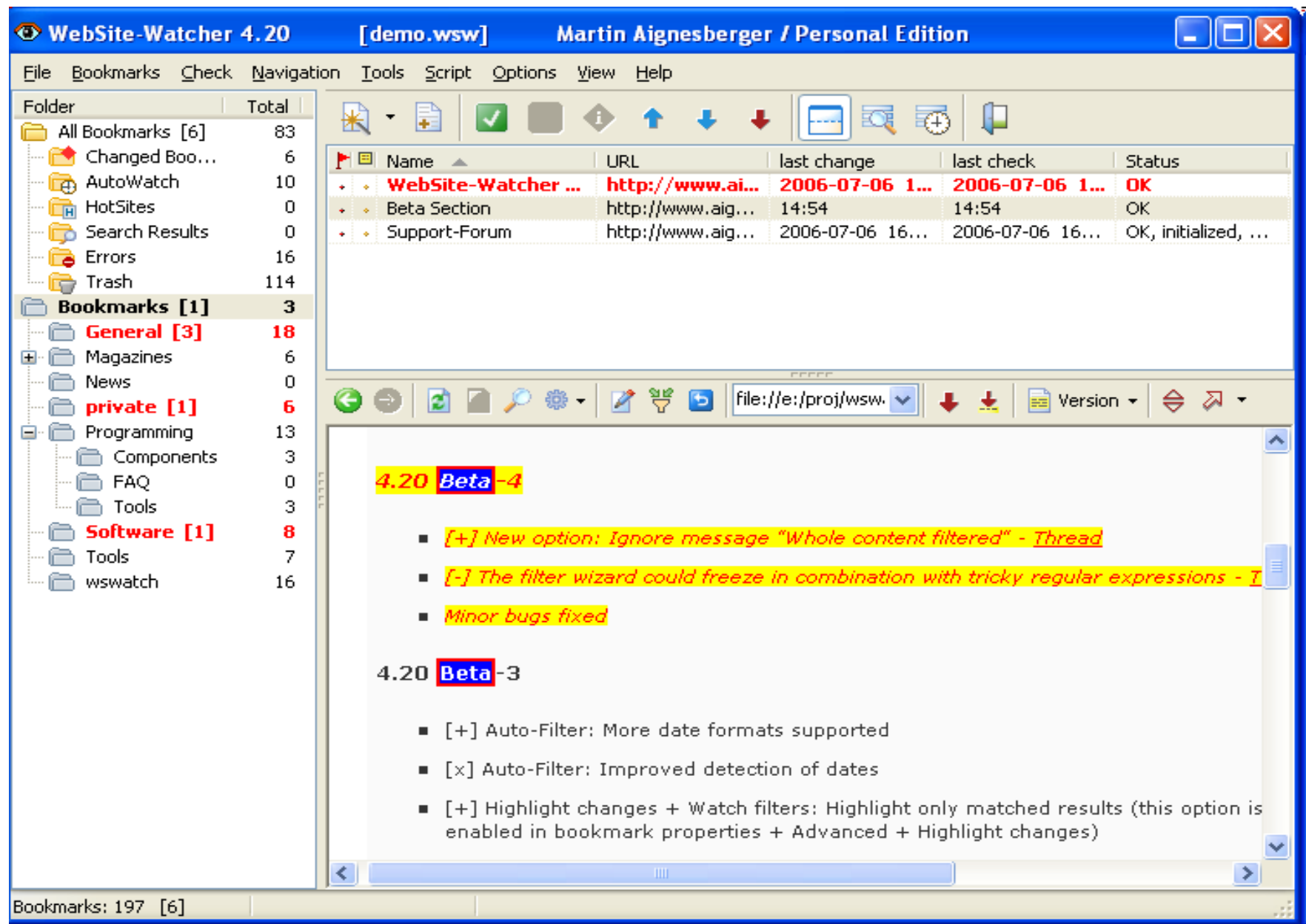
# Herramienta: SpiderFoot



# Herramienta: Power Email Collector



# Herramienta: WebSite Watcher





# ¿Qué es la Ingeniería Social?

- La ingeniería social es un método no técnico para obtener información sobre un sistema, basado en el factor humano, que puede ser utilizada antes o durante un ataque.
- Esto incluye el proceso de engañar a los usuarios, convenciéndolos de que den información que no deberían dar debido a su importancia o sensibilidad.
- La ingeniería social supone el uso de la influencia y persuasión, ya sea personalmente o vía teléfono, e-mail, etc.
- Los métodos tienden a explotar la tendencia natural de las personas a confiar y ayudar a otras personas.
- El uso de estos métodos deja bien claro que el usuario es el eslabón mas débil de la cadena en la seguridad.

# Comportamientos Vulnerables a Ataques

- **Confianza**

La confianza propia de la naturaleza humana es la base de cualquier ataque de la ingeniería social.

- **Ignorancia**

La ignorancia o subestimación sobre la ingeniería social y sus efectos hace de la organización un blanco fácil.

- **Miedo**

Advertencias y amenazas de graves peligros en caso del incumplimiento de la solicitud.

- **Codicia**

Promesas de algo por nada.

- **Deber moral**

Cumplimiento de lo solicitado por un sentido de obligación moral.

# Fases de la Ingeniería Social

- Investigación sobre la empresa/persona objetivo
  - Dumpster diving, sitios Web, empleados, visitas a la compañía y más.
- Seleccionar una víctima
  - Identificar empleados frustrados, disconformes, incrédulos, principiantes, etc.
- Desarrollar una relación
  - Desarrollo de una relación con determinados empleados.
- Explotar las relaciones para alcanzar el objetivo
  - Obtener información sensible sobre una cuenta.

# Información Sensible

- Un atacante desea obtener información sensible que de otra forma no podría averiguar, como por ejemplo:
  - Políticas de seguridad
  - Documentos clasificados
  - Infraestructura de red de la oficina
  - Contraseñas

# Tipos de Ataques Comunes

- Podemos dividir la ingeniería social en dos ramas:
  - Human-based: Referida a la interacción de persona a persona, directamente o de manera remota (ej: teléfono).
  - Computer-based: Referida al uso de software para interactuar con el usuario (ej: phishing).
- Una variante mas avanzada es la ingeniería social inversa, que implica que el usuario contacte al atacante “sin que este lo solicite”.

# Tipos de Ataques Comunes: Human Based

- **Impersonalización**

Ganar acceso físico simulando ser un usuario válido.

- **El empleado importante**

Simulación de ser un ejecutivo, gerente, director, etc. que necesita acción inmediata. Se usa la intimidación, ya que nadie cuestionaría a un superior en posición de autoridad.

- **La tercera parte de confianza**

Suponer la autorización de una tercera persona válida para simular un permiso en realidad inexistente.

# Tipos de Ataques Comunes: Human Based (Cont.)

- **El soporte técnico**

Simulación de ser personal técnico para la obtención de información.

- **Shoulder surfing**

Supone la obtención de contraseñas espiando lo que tpea un usuario al autenticarse.

- **Dumpster diving**

Buscar información escrita o impresiones en la basura.

# Tipos de Ataques Comunes: Computer Based

- Archivos adjuntos en e-mails
- Sitios web falsos
- Ventanas emergentes (popups)



# Tipos de Ataques Comunes: Objetivos Comunes

- Recepcionistas y personal de mesa de ayuda
- Ejecutivos de soporte técnico
- Proveedores de la organización
- Administradores de sistemas y usuarios

# Comprendiendo los Ataques Internos

- Si un hacker no puede averiguar nada sobre una organización, la alternativa será infiltrarse en la misma.
- De esta manera, se podría incluir en una búsqueda laboral o aprovechar algún empleado descontento que quiera colaborar.
- También se puede simular ser un empleado de limpieza, entrega de comida, guardia de seguridad, etc.
- Internamente el acceso a la información es mas directo y libre.
- Se estima que un 60% de los ataques ocurren desde adentro

# Comprendiendo los Ataques Internos (Cont.)

## ■ **Tailgating**

- Una persona no autorizada, con una credencial de identificación falsa, entra en una zona segura siguiendo de cerca a una persona autorizada que ingresa a través de una puerta que requiere clave de acceso.
- La persona autorizada desconoce que proporciona a una persona no autorizada el acceso a una zona restringida.

## ■ **Piggybacking**

- Una persona autorizada proporciona acceso a una persona no autorizada

# Comprendiendo los Ataques Internos (Cont.)

- **Eavesdropping**

- Escucha de conversaciones o lectura de mensajes de forma no autorizada.
- Cualquier forma de interceptación, como audio, vídeo o por escrito.

# Comprendiendo los Ataques Internos (Cont.)

- **Contramedidas para las amenazas internas**
  - Separación de las tareas
  - Rotación de las tareas
  - Mínimos privilegios
  - Control de acceso
  - Auditorías y logs
  - Política legal

# Comprendiendo el Robo de Identidad

- Un hacker podría hacer uso del robo de identidad para perpetrar un ataque.
- Las técnicas combinadas de recolección de información podrían permitir la creación de una identificación falsa.
- En organizaciones numerosas habrá mayores controles pero también mayor cantidad de personas, lo cual evita el reconocimiento directo.
- En organizaciones pequeñas, el reconocimiento personal es mas directo, por lo que se ejercen menos controles.

# Ataques de Phishing

- El phishing supone el envío de e-mails, normalmente simulando ser un banco o entidad financiera, en los cuales se requiere confirmación de datos o cualquier razón para justificar el acceso a un sistema online.
- Luego, es probable que la persona se dirija al sitio falso, normalmente mediante el click en un link adjunto.
- Si la persona ingresa sus datos, los estará proporcionando a un entidad falsa creyendo que es real.
- A continuación suele redireccionarse al usuario al sitio real para no levantar sospecha.

# Online Scams

- Algunos sitios web requieren una registración al usuario, y la aprovecha para tomar sus datos de manera real, para luego utilizarlos en otros servicios, dada la alta probabilidad de que se repitan los datos de acceso (usuario y/o password) elegidos.
- Los archivos adjuntos en e-mails pueden ser utilizados para enviar código malicioso de manera sencilla. Este es un tipo de ataque clásico y muy difundido.
- Las ventanas emergentes también pueden utilizarse de manera similar para ofrecer beneficios inexistentes, o sugiriendo la instalación de software malicioso.



# Ofuscación de URLs

- Las URL (Uniform Resource Locator) son utilizadas en la barra de direcciones del navegador para acceder a un sitio en particular.
- La ofuscación de URL implica esconder o falsear la URL real y se utiliza mayormente en ataques de phishing.
- Ejemplo:
  - **`http://200.42.111.56/bancoxxxx`**
  - **`http://secure.bancoxxxxx.dominiox.com`**
- La técnica puede incluir el uso de logos reales, pero con hipervínculos falsos, cuya dirección está ofuscada mediante distintas notaciones.

# Contramedidas

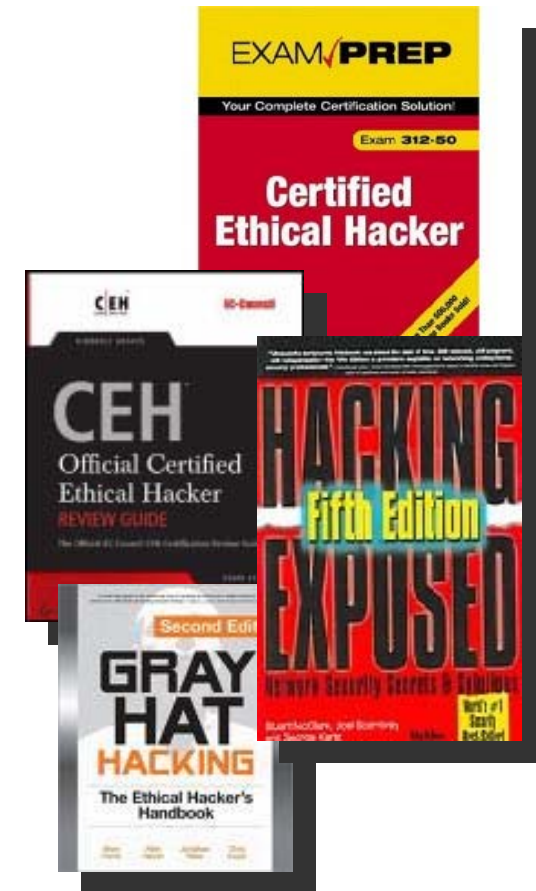
- No existe firewall, ni IDS, ni antivirus que proteja contra la ingeniería social dado que no es un ataque técnico.
- Las correctas políticas y procedimientos de seguridad pueden mitigar los ataques de ingeniería social.
- Los programas de concientización (awareness) son sin duda la mejor herramienta para ayudar a evitar que los empleados sean víctimas de este tipo de ataques.

# **Footprinting e Ingeniería Social**

Links, Referencias y  
Lecturas Complementarias

# Referencias y Lecturas Complementarias

- **CEH Official Certified Ethical Hacker Review Guide**  
By Kimberly Graves  
(Sybex) ISBN: 0782144373
- **Certified Ethical Hacker Exam Prep**  
By Michael Gregg  
(Que) ISBN: 0789735318
- **Hacking Exposed, Fifth Edition**  
By S.McClure, J.Scambray, and G.Kurtz  
(McGraw-Hill Osborne Media) ISBN: 0072260815
- **Gray Hat Hacking, Second Edition**  
By S.Harris, A.Harper, C.Eagle, J.Ness  
(McGraw-Hill Osborne Media) ISBN: 0071495681



# **Footprinting e Ingeniería Social**

Preguntas?