

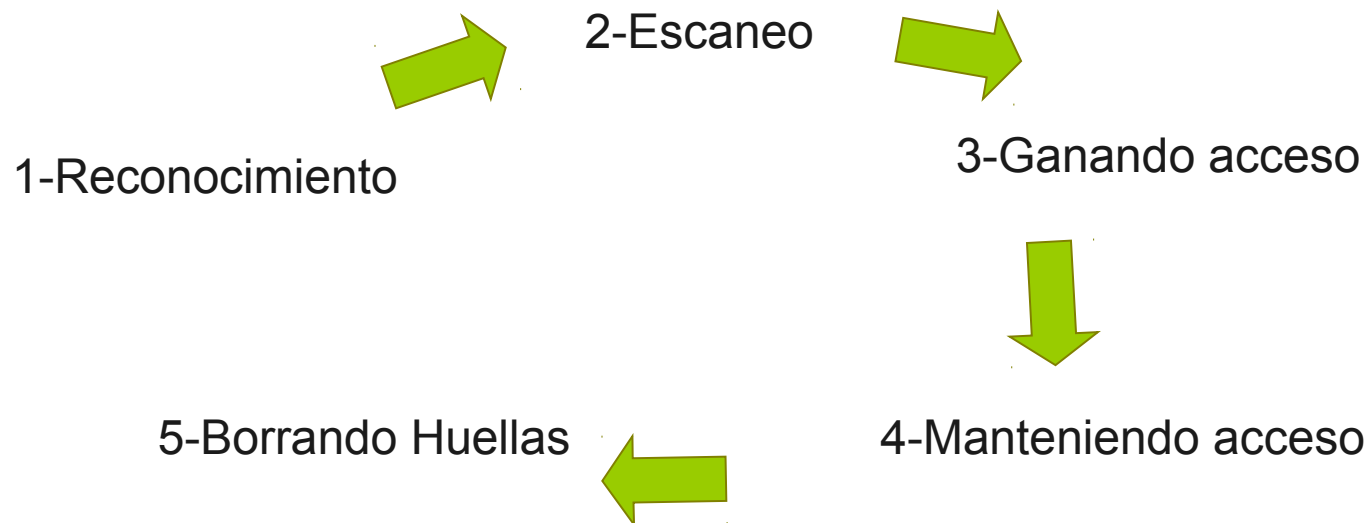
# Seguridad y Privacidad en Redes

Técnicas de descubrimiento:  
Obteniendo información de la  
red



# Obteniendo información de la red...

## Fases de un ataque



# Obteniendo información de la red...

## Reconocimiento..Obteniendo datos

Se llama reconocimiento a la fase de preparación del ataque, en la cual se busca obtener la mayor cantidad de información posible sobre el objetivo, previo a hacer efectivo el ataque.

El reconocimiento puede ser:

- Pasivo
- Activo



# Técnicas de descubrimiento

Se utilizan para obtener la mayor cantidad de información posible sobre el objetivo, en la fase de preparación del ataque.

- Footprinting
- Enumeración
- Fingerprinting
- Escaneo de puertos
- Escaneo de vulnerabilidades



# Footprinting

Se recolecta información de la organización usando métodos no intrusivos.

Se vale de información pública disponible en la página WEB, a través de consultas de DNS, a través de requerimientos de WHOIS, etc

La información resultante (números de TEL, direcciones, direcciones IP, direcciones de mail) es obtenida de forma legal.



# Footprinting

## Mecanismos y Herramientas:

**Sitio Web de la organización**

**Consultas de WHOIS**

**Entidades de asignación de nombre de DNS: nic.ar**

**Consultas de DNS**

**Webarchive**

***Netcraft***

**Buscadores -> Googlehacking**

**... etc.**



# Consultas WHOIS

nicolas@poseidon:~\$ whois 64.233.169.99

OrgName: Google Inc.  
OrgID: G0GL  
Address: 1600 Amphitheatre Parkway  
City: Mountain View  
StateProv: CA  
PostalCode: 94043  
Country: US

NetRange: 64.233.160.0 - 64.233.191.255  
CIDR: 64.233.160.0/19  
NetName: GOOGLE  
NetHandle: NET-64-233-160-0-1  
Parent: NET-64-0-0-0-0  
NetType: Direct Allocation  
NameServer: NS1.GOOGLE.COM  
NameServer: NS2.GOOGLE.COM  
NameServer: NS3.GOOGLE.COM  
NameServer: NS4.GOOGLE.COM  
Comment:  
RegDate: 2003-08-18  
Updated: 2007-04-10

RTechHandle: ZG39-ARIN  
RTechName: Google Inc.  
RTechPhone: +1-650-318-0200  
RTechEmail: arin-contact@google.com

OrgTechHandle: ZG39-ARIN  
OrgTechName: Google Inc.  
OrgTechPhone: +1-650-318-0200  
OrgTechEmail: arin-contact@google.com



# Entidades de asignación de DNS

NIC.ar network information center argentina	
Consulta de dominios	<b>Consulta de Dominios</b>
Registrar dominio	El dominio <b>laserenisima.com.ar</b> se encuentra registrado desde el 01/01/1996.
Renovar dominio	Fecha de vencimiento: 01/01/2009
Transferir dominio	<b>Entidad Registrante:</b> MASTELLONE HNOS S.A.
Trámites vía web	País: Argentina
Registro escalonado	Actividad: Productos Alimenticios.
Dominios .edu.ar	<b>Datos en Argentina</b>
Guía del solicitante	Domicilio: Encarnacion Ezcurra 365 piso 2 oficina 310
Normativa vigente	Ciudad/Localidad: Ciudad de Buenos Aires
Preguntas frecuentes	Provincia: Ciudad de Buenos Aires
Glosario de términos	Código Postal: C1107CLA
Guías interactivas	Teléfono: 0237-4859000
Vías de contacto	Fax: 0237-4859175
<b>NIC Argentina</b> Esmeralda 1212, C1007ABR Buenos Aires - Argentina Tel.: +54 (11) 4819-7631 Fax: +54 (11) 4819-7630 e-mail: info@nic.ar	<b>Persona Responsable:</b> Ezequiel Basombrío
	Domicilio: Encarnacion Ezcurra 365 2 31
Ministerio de Relaciones Exteriores, Comercio Internacional y Culto	Ciudad: Capital Federal
	Código Postal: C1107CLA
	Provincia: Ciudad de Buenos Aires
	País: Argentina
	Teléfono: 0237-4859000
	Fax: 0237-4859175
	Horario de contacto: 9 a 18 hs.





# Entidades de asignación de DNS

**Entidad Administradora:** Global Crossing Argentina S.A.

**Domicilio:** Alferez Pareja 256

**Ciudad:** Ciudad de Buenos Aires

**Código Postal:** C1107BJD

**Provincia:** Ciudad de Buenos Aires

**País:** Argentina

**Teléfono:** 5170-6000

**Fax:** 5170-6000

**Actividad:** Telecomunicaciones

**Contacto Técnico:** Martegani, Diego

**Domicilio:** Alferez Pareja 256

**Ciudad:** Ciudad de Buenos Aires

**Código Postal:** C1107BJD

**Provincia:** Ciudad de Buenos Aires

**País:** Argentina

**Teléfono:** 5170-6572

**Fax:** 5170-6557

**Horario de contacto:** 9 a 18 hs.

**Servidores DNS:**

**DNS Primario:** *Nombre:* ns1.impsat.net.ar

*Dirección IP:* 200.0.194.44

**DNS Secundario:** *Nombre:* ns2.impsat.net.ar

*Dirección IP:* 200.31.1.86



# Consultas de DNS

```
nicolas@poseidon:~$ dig www.google.com
```

```
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.                500583  IN      CNAME   www.l.google.com.
www.l.google.com.              282     IN      A        64.233.169.104
www.l.google.com.              282     IN      A        64.233.169.103
www.l.google.com.              282     IN      A        64.233.169.99
www.l.google.com.              282     IN      A        64.233.169.147

;; AUTHORITY SECTION:
l.google.com.                  74116   IN      NS       d.l.google.com.
l.google.com.                  74116   IN      NS       g.l.google.com.
l.google.com.                  74116   IN      NS       b.l.google.com.
l.google.com.                  74116   IN      NS       h.l.google.com.
l.google.com.                  74116   IN      NS       c.l.google.com.
l.google.com.                  74116   IN      NS       f.l.google.com.
l.google.com.                  74116   IN      NS       e.l.google.com.
l.google.com.                  74116   IN      NS       a.l.google.com.

;; ADDITIONAL SECTION:
b.l.google.com.                49941   IN      A        64.233.179.9
c.l.google.com.                74310   IN      A        64.233.161.9
d.l.google.com.                74241   IN      A        66.249.93.9
h.l.google.com.                11143   IN      A        74.125.45.9
f.l.google.com.                28934   IN      A        72.14.235.9
a.l.google.com.                1145    IN      A        209.85.139.9
g.l.google.com.                83667   IN      A        74.125.95.9
e.l.google.com.                51288   IN      A        209.85.137.9
```



# Consultas de DNS

```
nicolas@poseidon:~$ dig -t ns google.com

; <>> DiG 9.4.2-P1 <>> -t ns google.com
;; global options: printcmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 43749
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 4

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

;; ANSWER SECTION:
google.com.                 164342  IN      NS      ns3.google.com.
google.com.                 164342  IN      NS      ns1.google.com.
google.com.                 164342  IN      NS      ns4.google.com.
google.com.                 164342  IN      NS      ns2.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.             76110   IN      A        216.239.32.10
ns2.google.com.             76110   IN      A        216.239.34.10
ns3.google.com.             69341   IN      A        216.239.36.10
ns4.google.com.             76110   IN      A        216.239.38.10

;; Query time: 26 msec
;; SERVER: 200.63.155.75#53(200.63.155.75)
;; WHEN: Thu Oct 9 20:29:43 2008
;; MSG SIZE rcvd: 164
```



# Consultas de DNS

```
nicolas@poseidon:~$ dig -t soa google.com
```

```
; <<>> DiG 9.4.2-P1 <<>> -t soa google.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64278
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
google.com.                IN      SOA

;; ANSWER SECTION:
google.com.                86400   IN      SOA      ns1.google.com. dns-admin.google.com. 2008100800 7200 1800 1209600 300

;; AUTHORITY SECTION:
google.com.                79376   IN      NS       ns2.google.com.
google.com.                79376   IN      NS       ns1.google.com.
google.com.                79376   IN      NS       ns3.google.com.
google.com.                79376   IN      NS       ns4.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.            68914   IN      A        216.239.32.10
ns2.google.com.            68914   IN      A        216.239.34.10
ns3.google.com.            68914   IN      A        216.239.36.10
ns4.google.com.            68914   IN      A        216.239.38.10

;; Query time: 219 msec
;; SERVER: 200.63.155.75#53(200.63.155.75)
;; WHEN: Thu Oct 9 20:31:04 2008
;; MSG SIZE rcvd: 210
```



# Consultas de DNS

```

nicolas@poseidon:~$ dig -t mx google.com

; <>> DiG 9.4.2-P1 <>> -t mx google.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32430
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 4, ADDITIONAL: 8

;; QUESTION SECTION:
google.com.                IN      MX

;; ANSWER SECTION:
google.com.                574     IN      MX      10 smtp4.google.com.
google.com.                574     IN      MX      10 smtp1.google.com.
google.com.                574     IN      MX      10 smtp2.google.com.
google.com.                574     IN      MX      10 smtp3.google.com.

;; AUTHORITY SECTION:
google.com.                75659   IN      NS      ns1.google.com.
google.com.                75659   IN      NS      ns2.google.com.
google.com.                75659   IN      NS      ns3.google.com.
google.com.                75659   IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
smtp1.google.com.          1359    IN      A        209.85.237.25
smtp2.google.com.          267     IN      A        64.233.165.25
smtp3.google.com.          1669    IN      A        64.233.183.25
smtp4.google.com.          922     IN      A        72.14.221.25
ns1.google.com.            134965  IN      A        216.239.32.10
ns2.google.com.            129998  IN      A        216.239.34.10
ns3.google.com.            129998  IN      A        216.239.36.10
ns4.google.com.            135085  IN      A        216.239.38.10

```



# Google hacking

Utilizando a google para obtener información mediante su motor de búsqueda



# Google hacking

## ¿Qué podemos encontrar?!

- Productos WEB con vulnerabilidades conocidas.
- Mensajes de error.
- Archivos con información sensible.
- Páginas con formularios de acceso.
- Listados de directorios.
- Interfaces de administración de dispositivos de
- Hardware (cámaras web por ejemplo).





# Google hacking

Web [Images](#) [Maps](#) [News](#) [Shopping](#) [Gmail](#) [more ▼](#)

[Sign in](#)



[Advanced Search](#)  
[Preferences](#)

Web

Results **1 - 10** of about **387** from **unlp.edu.ar** for **filetype:xls**. (0.09 seconds)

**[xls]** [Hoja1](#)

File Format: Microsoft Excel - [View as HTML](#)

A, B, C. 1, UNIVERSIDAD NACIONAL DE LA PLATA. 2, FACULTAD DE CIENCIAS ECONOMICAS . 3, SECRETARIA DE EXTENSION UNIVERSITARIA ...

[www.econo.unlp.edu.ar/entrevistaEcoRadio2007.xls](http://www.econo.unlp.edu.ar/entrevistaEcoRadio2007.xls) - [Similar pages](#)

**[xls]** [IDENTIFICACION](#)

File Format: Microsoft Excel

A, B, C. 1, Nombre:. 2, Apellido:. 3, DNI/CEDULA/LC :. 4, Email:. 5, Teléfono:. 6, Institucion. 7, Principal actividad desempeñada ...

[www.roble.unlp.edu.ar/textos/SECYT\\_Listado\\_encuesta.xls](http://www.roble.unlp.edu.ar/textos/SECYT_Listado_encuesta.xls) - [Similar pages](#)

**[xls]** [TFIndus](#)

File Format: Microsoft Excel - [View as HTML](#)

A, B, C, D, E, F, G, H. 1, NUMERO, TITULO, SUBTITULO, AUTOR/ES, RESPONSABLE/S, TEMAS, FECHA, UBICACION. 2, Trabajo Final de Ingeniería Industrial; 1 ...

[www.ing.unlp.edu.ar/bibcent/indus.xls](http://www.ing.unlp.edu.ar/bibcent/indus.xls) - [Similar pages](#)

**[xls]** [Datos 2004](#)

File Format: Microsoft Excel - [View as HTML](#)

A, B, C, D, E, F, G. 1, Proyecto ROBLE Bibliotecas de la UNLP. 2, ETI Evaluacion de unidades de informacion. 3, Formulario estadístico normalizado 2004 ...

[www.roble.unlp.edu.ar/textos/ETIEVA\\_formu04.xls](http://www.roble.unlp.edu.ar/textos/ETIEVA_formu04.xls) - [Similar pages](#)

**[xls]** [Hoja1](#)

File Format: Microsoft Excel - [View as HTML](#)

A, B, C, D, E. 1. 2, UNIVERSIDAD NACIONAL DE LA PLATA - DEPARTAMENTO DE CIENCIAS ADMINISTRATIVAS - año 2005. 3, Seminario Taller: Administración y ...

[www.econo.unlp.edu.ar/cursos/administracion\\_y\\_administradores\\_para\\_el\\_siglo\\_xxi.xls](http://www.econo.unlp.edu.ar/cursos/administracion_y_administradores_para_el_siglo_xxi.xls) - [Similar pages](#)

**[xls]** [TFElectro](#)

File Format: Microsoft Excel - [View as HTML](#)

A, B, C, D, E, F, G. 1, NUMERO, TITULO, AUTOR/ES, RESPONSABLE, TEMAS, FECHA. 2, Trabajo Final de Electrónica ; 1, Medidor de energía con tarifa programable ...

[www.ing.unlp.edu.ar/bibcent/electro.xls](http://www.ing.unlp.edu.ar/bibcent/electro.xls) - [Similar pages](#)

**[xls]** [Formulario](#)

File Format: Microsoft Excel - [View as HTML](#)

A, B, C, D, E, F, G, H, I, J. 1, Proyecto ROBLE: Bibliotecas de la UNLP. 2, Formulario estadístico año 2001. 3. 4. 5, DATOS DE IDENTIFICACION ...

[www.roble.unlp.edu.ar/textos/ETIEVA\\_formu01.xls](http://www.roble.unlp.edu.ar/textos/ETIEVA_formu01.xls) - [Similar pages](#)

**[xls]** [GUC](#)

File Format: Microsoft Excel - [View as HTML](#)

4, 5, OBRA, UNIDAD ACADEMICA, UBICACIÓN, FUENTE DE FINANCIAMIENTO, MONTO (pesos) , ESTADO, SUPERFICIE m2, OBSERVACIONES ...

[www.unlp.edu.ar/uploads/docs/obrasguccorr.xls](http://www.unlp.edu.ar/uploads/docs/obrasguccorr.xls) - [Similar pages](#)

**[xls]** [Hoja1](#)

File Format: Microsoft Excel - [View as HTML](#)

A, B, C, D, E, F. 1, V - Cursograma de Rendición de Subsidios. 2, Unidad Académica, UNLP, UNLP. 3, Secretaría otorgante, Director del Proyecto ...

[www.unlp.edu.ar/uploads/docs/cursograma\\_rendiciones.xls](http://www.unlp.edu.ar/uploads/docs/cursograma_rendiciones.xls) - [Similar pages](#)



# Google hacking

Ejemplos: Productos vulnerables



**PHP Version 4.4.1**



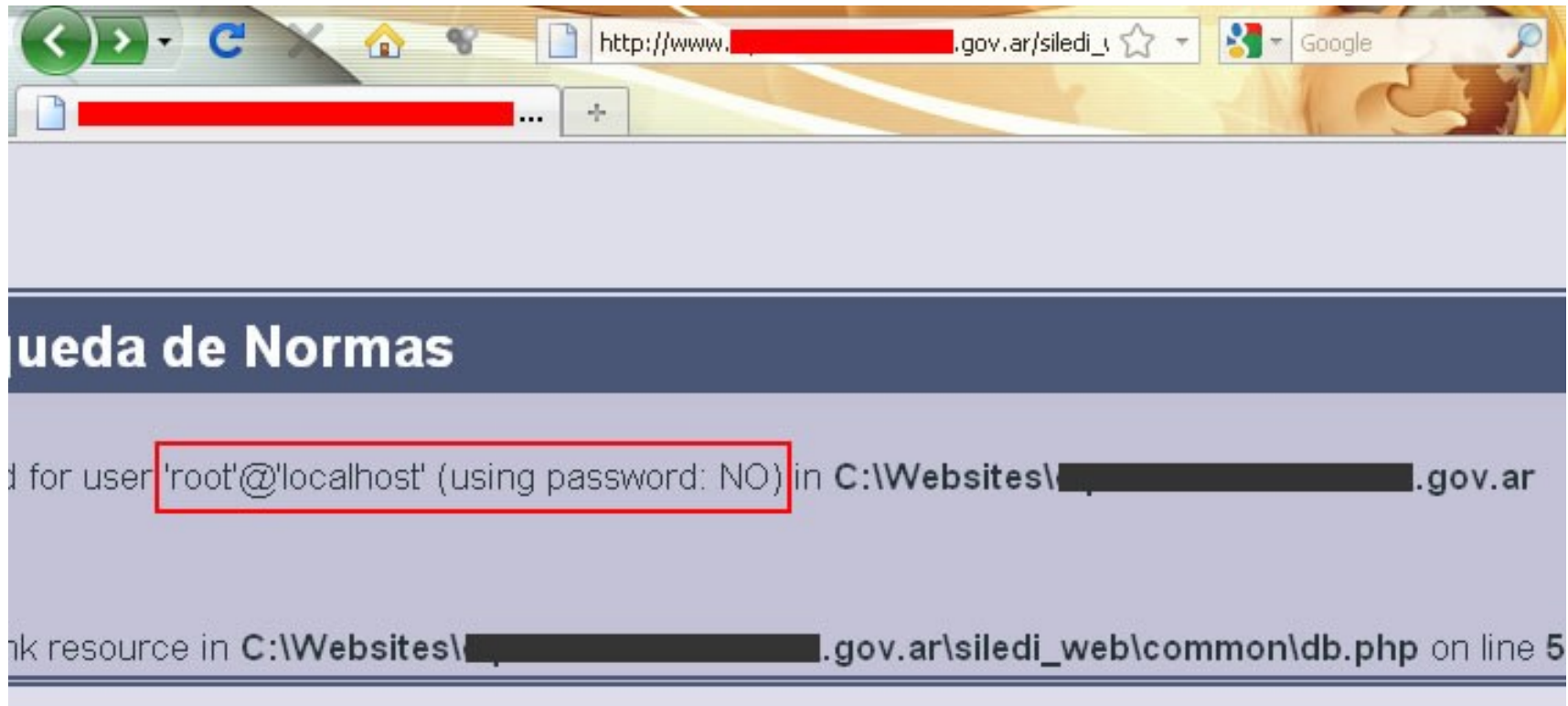
<b>System</b>	Linux whdlx17 2.6.9-5.ELsmp #1 SMP Wed Jan 5 19:30:39 EST 2005 i686
<b>Build Date</b>	Dec 25 2005 23:10:16
<b>Configure Command</b>	'./configure' '--prefix=/opt/php/4.4.1' '--with-mysql=/opt/mysql' '--with-apxs=/opt/apache/1.3.34/bin/apxs' '--with-gd=/opt/gd/2.0.33' '--with-zlib-dir=/opt/zlib/1.2.3'
<b>Server API</b>	Apache
<b>Virtual Directory Support</b>	disabled
<b>Configuration File (php.ini) Path</b>	/opt/php/4.4.1/lib/php.ini
<b>PHP API</b>	20020918
<b>PHP Extension</b>	20020429

inurl:gov.ar + intext:phpinfo



# Google hacking

Ejemplos: Mensajes de error



intext:"access denied for user" "using password" inurl:gov.ar



# Google hacking

Ejemplos: Archivos con nombres de usuarios



Agents | Locations | Load History | Truck History | Roll Loads | Roll Trucks | | Login

HOME PAGE  
AVAILABLE LOADS  
AVAILABLE TRUCKS

## AGENTS

Total  
Agents: 66

<u>First Name</u>	<u>Last Name</u>	<u>Phone</u>	<u>Email</u>	<u>Location</u>
JOHN	[redacted]	936-890-[redacted]	[redacted]@keystonelogistics.net	KEYSTONE LOGISTICS WILLIS, TX
Michael	[redacted]	479-649-[redacted]	[redacted]@transportleasing.com	TLI - Ft Smith, AR
BART	[redacted]	877-778-[redacted]	[redacted]@keystonelogistics.net	Keystone Logistics, SBN
Dale	[redacted]	877-301-[redacted]	[redacted]@bellsouth.net	Keystone Line Gadsden

inurl:admin inurl:userlist



# Google hacking

Ejemplos: Páginas con formularios de acceso



The screenshot shows a web browser window with the address bar displaying `http://www.[redacted].gov.ar/novedades/wp-login`. The browser's address bar also shows a tab titled "WordPress > Entrar". The main content area displays the WordPress login form, which includes the WordPress logo, a "Nombre de usuario:" label with a text input field, a "Contraseña:" label with a password input field, a "Remember me" checkbox, and an "Entrar >>" button. At the bottom of the form, there are two links: "« Volver al weblog" and "¿Olvidó su contraseña?".

`inurl:gov.ar inurl:wp-login.php`





## WEB.ARCHIVE.ORG

Enter Web Address: 

All

[Take Me Back](#)[Adv. Search](#) [Compare Archive Pages](#)Searched for <http://www.google.com>

3615 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 - Apr 12, 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	24 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="#">Mar 25, 2008</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="#">Mar 26, 2008</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="#">Apr 01, 2008</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="#">Jun 09, 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 13, 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> *	

# WEB.ARCHIVE.ORG



Search the web using Google!

Google Search

I'm feeling lucky

Special Searches

[Stanford Search](#)

[Linux Search](#)

[Why use Google!](#)

[Press about Google!](#)

[Help!](#)

[Company Info](#)

[Jobs at Google](#)

[Google! Logos](#)

[Making Google! the Default](#)

Get Google!  
updates monthly:

your e-mail

Subscribe

[Archive](#)

Copyright ©1999 Google Inc.

[www.google.com](http://www.google.com) / 17 de Enero de 1999







# Netcraft

UNLP - FACULTAD DE INFORMÁTICA - LINTI



Site Search

## Search Web by Domain

Explore 6,534,940 web sites visited by users of the [Netcraft Toolbar](#)

9th October 2008

Search:

[search tips](#)

site contains

.google.com

lookup!

example: site contains .sco.com

## Results for .google.com

Found 432 sites

	Site	Site Report	First seen	Netblock	OS
1.	<a href="http://www.google.com">www.google.com</a>		November 1998	<a href="#">Google Inc.</a>	<a href="#">Linux</a>
2.	<a href="http://mail.google.com">mail.google.com</a>		June 2004	<a href="#">Google Inc.</a>	<a href="#">Linux</a>
3.	<a href="http://images.google.com">images.google.com</a>		November 2001	<a href="#">Google Inc.</a>	<a href="#">Linux</a>
4.	<a href="http://news.google.com">news.google.com</a>		April 2002	<a href="#">Google Inc.</a>	<a href="#">Linux</a>
5.	<a href="http://www.google.com.br">www.google.com.br</a>		March 2002	<a href="#">Google Inc.</a>	<a href="#">Linux</a>
6.	<a href="http://www.google.com.au">www.google.com.au</a>		August 1999	<a href="#">Google Inc.</a>	<a href="#">Linux</a>
7.	<a href="http://maps.google.com">maps.google.com</a>		April 2005	<a href="#">Google Inc.</a>	<a href="#">Linux</a>
8.	<a href="http://groups.google.com">groups.google.com</a>		March 2001	<a href="#">Google Inc.</a>	<a href="#">Linux</a>
9.	<a href="http://groups-beta.google.com">groups-beta.google.com</a>		July 2004	<a href="#">Google Inc.</a>	<a href="#">Linux</a>
10.	<a href="http://www.google.com.mx">www.google.com.mx</a>		July 2002	<a href="#">Google Inc.</a>	<a href="#">Linux</a>
11.	<a href="http://translate.google.com">translate.google.com</a>		November 2001	<a href="#">Google Inc.</a>	<a href="#">Linux</a>
12.	<a href="http://www.google.com.ar">www.google.com.ar</a>		August 1999	<a href="#">Google Inc.</a>	<a href="#">Linux</a>
13.	<a href="http://www.google.com.gr">www.google.com.gr</a>		January 2003	<a href="#">Google Inc.</a>	<a href="#">Linux</a>
14.	<a href="http://www.google.com.sg">www.google.com.sg</a>		December 2002	<a href="#">Google Inc.</a>	<a href="#">Linux</a>
15.	<a href="http://desktop.google.com">desktop.google.com</a>		December 2004	<a href="#">Google Inc.</a>	<a href="#">Linux</a>



## Site report for www.google.com

### Netcraft Toolbar

- [Home](#)
- [Download Now!](#)
- [Report a Phish](#)
- [Tell a Friend](#)
- [Top Reporters](#)
- [Phishiest Countries](#)
- [Phishiest Hosters](#)
- [Most Popular Websites](#)
- [Branded Toolbars](#)

 [→](#)




### Toolbar Support

- [FAQ](#)
- [Glossary](#)
- [Contact Us](#)
- [Report a Bug](#)

### Tutorials

- [Installing the Toolbar](#)
- [Using the Toolbar](#)
- [Getting the Most](#)
- [Reporting a Phish](#)
- [Configuration](#)

### About Netcraft

<b>Site</b>	<a href="http://www.google.com">http://www.google.com</a>	<b>Last reboot</b>	275 days ago  <a href="#">Uptime graph</a>
<b>Domain</b>	<a href="http://google.com">google.com</a>	<b>Netblock owner</b>	<a href="#">Google Inc.</a>
<b>IP address</b>	64.233.183.103	<b>Site rank</b>	1
<b>Country</b>	 US	<b>Nameserver</b>	ns1.google.com
<b>Date first seen</b>	November 1998	<b>DNS admin</b>	dns-admin@google.com
<b>Domain Registry</b>	markmonitor.com	<b>Reverse DNS</b>	nf-in-f103.google.com
<b>Organisation</b>	Google Inc., Please contact contact-admin@google.com 1600 Amphitheatre Parkway, United States	<b>Nameserver Organisation</b>	Google Inc., Please contact contact-admin@google.com 1600 Amphitheatre Parkway, United States
<b>Check another site:</b>	<input type="text"/>	<b>Netcraft Site Report Gadget</b>	 <a href="#">[More Netcraft Gadgets]</a>

### Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
<a href="#">Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043</a>	64.233.183.99	Linux	gws	1-Oct-2008
<a href="#">Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043</a>	64.233.183.99	Linux	gws	30-Sep-2008
<a href="#">Google Inc</a>	66.102.9.99	Linux	gws	29-Sep-2008
<a href="#">Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043</a>	64.233.183.103	Linux	gws	25-Sep-2008
<a href="#">Google Inc</a>	66.102.9.99	Linux	gws	24-Sep-2008
<a href="#">Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043</a>	64.233.183.99	Linux	gws	19-Sep-2008
<a href="#">Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043</a>	66.249.91.99	Linux	gws	18-Sep-2008
<a href="#">Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043</a>	64.233.183.99	Linux	gws	26-Aug-2008
<a href="#">Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043</a>	66.249.93.99	Linux	gws	25-Aug-2008
<a href="#">Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043</a>	64.233.183.99	Linux	gws	7-Aug-2008





# Enumeración

Permite obtener y recolectar información de máquinas, redes, aplicaciones, servicios, usuarios y/o otras tecnologías utilizadas y ofrecidas por una organización.

No se considera un ataque, pues sólo pretende recopilar de manera organizada información disponible mediante reiteradas consultas.

El objetivo es utilizar la información para planificar mejor el ataque.





# Enumeración - DNS

```
bt dnsenum1.1.1.Beta # ./dnsenum.pl -f dns.txt info.unlp.edu.ar  
./dnsenum.pl VERSION:1.1.1 Beta
```

```
----- info.unlp.edu.ar -----
```

```
-----  
Host's addresses:  
-----
```

```
-----  
Nameservers:  
-----
```

```
ada.info.unlp.edu.ar. 22349 IN A 163.10.5.66
```

```
-----  
MX record:  
-----
```

```
ada.info.unlp.edu.ar. 22349 IN A 163.10.5.66  
anubis.unlp.edu.ar. 23067 IN A 163.10.0.65
```

```
-----  
Trying Zonetransfers:  
-----
```

```
trying zonetransfer for info.unlp.edu.ar on ada.info.unlp.edu.ar ...
```

```
-----  
Brute forcing with dns.txt:  
-----
```

```
intranet.info.unlp.edu.ar. 85734 IN CNAME biblioteca.info.unlp.edu.ar.  
biblioteca.info.unlp.edu.ar. 85734 IN A 163.10.5.69  
mail.info.unlp.edu.ar. 15270 IN CNAME ada.info.unlp.edu.ar.  
ada.info.unlp.edu.ar. 22348 IN A 163.10.5.66  
sql.info.unlp.edu.ar. 85734 IN A 163.10.5.76  
www.info.unlp.edu.ar. 17768 IN CNAME web.info.unlp.edu.ar.  
web.info.unlp.edu.ar. 17768 IN A 163.10.34.99
```

```
-----  
info.unlp.edu.ar c class netranges:  
-----
```

```
163.10.5.0/24  
163.10.34.0/24
```

```
-----  
Performing reverse lookup on 512 ip addresses:  
-----
```

```
1.0-63.5.10.163.in-addr.arpa. 7531 IN PTR ns1.lfia.info.unlp.edu.ar.  
2.0-63.5.10.163.in-addr.arpa. 7578 IN PTR ns2.lfia.info.unlp.edu.ar.  
5.0-63.5.10.163.in-addr.arpa. 7607 IN PTR biblioteca.lfia.info.unlp.edu.ar.  
6.0-63.5.10.163.in-addr.arpa. 7608 IN PTR soporte.lfia.info.unlp.edu.ar.  
10.0-63.5.10.163.in-addr.arpa. 7614 IN PTR rrrh.lfia.info.unlp.edu.ar.  
11.0-63.5.10.163.in-addr.arpa. 7617 IN PTR calefon.lfia.info.unlp.edu.ar.  
13.0-63.5.10.163.in-addr.arpa. 7620 IN PTR neuquina.lfia.info.unlp.edu.ar.  
14.0-63.5.10.163.in-addr.arpa. 7622 IN PTR firewall.lfia.info.unlp.edu.ar.  
16.0-63.5.10.163.in-addr.arpa. 7625 IN PTR catedras.lfia.info.unlp.edu.ar.  
19.0-63.5.10.163.in-addr.arpa. 7631 IN PTR webseaside.lfia.info.unlp.edu.ar.  
24.0-63.5.10.163.in-addr.arpa. 17737 IN PTR sol.lfia.info.unlp.edu.ar.  
41.0-63.5.10.163.in-addr.arpa. 7680 IN PTR groupfia.lfia.info.unlp.edu.ar.  
65.5.10.163.in-addr.arpa. 86400 IN PTR hot.info.unlp.edu.ar.  
66.5.10.163.in-addr.arpa. 86400 IN PTR ada.info.unlp.edu.ar.  
67.5.10.163.in-addr.arpa. 86400 IN PTR proxy.info.unlp.edu.ar.  
68.5.10.163.in-addr.arpa. 86400 IN PTR biblio0.info.unlp.edu.ar.  
69.5.10.163.in-addr.arpa. 86400 IN PTR biblioteca.info.unlp.edu.ar.  
70.5.10.163.in-addr.arpa. 86400 IN PTR switch.info.unlp.edu.ar.  
71.5.10.163.in-addr.arpa. 86400 IN PTR switchgerman.info.unlp.edu.ar.  
71.5.10.163.in-addr.arpa. 86400 IN PTR pll.info.unlp.edu.ar.  
72.5.10.163.in-addr.arpa. 86400 IN PTR clu.info.unlp.edu.ar.  
73.5.10.163.in-addr.arpa. 86400 IN PTR extension.info.unlp.edu.ar.  
74.5.10.163.in-addr.arpa. 86400 IN PTR prueba.info.unlp.edu.ar.  
75.5.10.163.in-addr.arpa. 86400 IN PTR biotec.info.unlp.edu.ar.  
76.5.10.163.in-addr.arpa. 86400 IN PTR sql.info.unlp.edu.ar.  
77.5.10.163.in-addr.arpa. 86400 IN PTR fortran.info.unlp.edu.ar.  
78.5.10.163.in-addr.arpa. 86400 IN PTR basic.info.unlp.edu.ar.  
79.5.10.163.in-addr.arpa. 86400 IN PTR rpg.info.unlp.edu.ar.  
80.5.10.163.in-addr.arpa. 86400 IN PTR cpp.info.unlp.edu.ar.  
81.5.10.163.in-addr.arpa. 86400 IN PTR modula.info.unlp.edu.ar.  
82.5.10.163.in-addr.arpa. 86400 IN PTR tcl.info.unlp.edu.ar.  
83.5.10.163.in-addr.arpa. 86400 IN PTR prolog.info.unlp.edu.ar.  
84.5.10.163.in-addr.arpa. 86400 IN PTR lisp.info.unlp.edu.ar.  
85.5.10.163.in-addr.arpa. 86400 IN PTR dylan.info.unlp.edu.ar.  
86.5.10.163.in-addr.arpa. 86400 IN PTR tito.info.unlp.edu.ar.  
87.5.10.163.in-addr.arpa. 86400 IN PTR server-finio.info.unlp.edu.ar.  
89.5.10.163.in-addr.arpa. 86400 IN PTR grid-unlp.info.unlp.edu.ar.  
90.5.10.163.in-addr.arpa. 86400 IN PTR webinfo.info.unlp.edu.ar.  
91.5.10.163.in-addr.arpa. 86400 IN PTR ada2.info.unlp.edu.ar.  
92.5.10.163.in-addr.arpa. 86400 IN PTR auxiliar.info.unlp.edu.ar.  
94.5.10.163.in-addr.arpa. 86400 IN PTR pc-router.info.unlp.edu.ar.  
101.5.10.163.in-addr.arpa. 86400 IN PTR dgcm.info.unlp.edu.ar.  
102.5.10.163.in-addr.arpa. 86400 IN PTR pc-linti.info.unlp.edu.ar.  
121.5.10.163.in-addr.arpa. 86400 IN PTR secinf.info.unlp.edu.ar.  
122.5.10.163.in-addr.arpa. 86400 IN PTR anexa.info.unlp.edu.ar.  
126.5.10.163.in-addr.arpa. 86400 IN PTR router2.info.unlp.edu.ar.  
130.5.10.163.in-addr.arpa. 86400 IN PTR mac130.info.unlp.edu.ar.  
131.5.10.163.in-addr.arpa. 86400 IN PTR mac131.info.unlp.edu.ar.  
132.5.10.163.in-addr.arpa. 86400 IN PTR mac132.info.unlp.edu.ar.  
133.5.10.163.in-addr.arpa. 86400 IN PTR mac133.info.unlp.edu.ar.  
134.5.10.163.in-addr.arpa. 86400 IN PTR mac134.info.unlp.edu.ar.  
135.5.10.163.in-addr.arpa. 86400 IN PTR mac135.info.unlp.edu.ar.  
136.5.10.163.in-addr.arpa. 86400 IN PTR mac136.info.unlp.edu.ar.  
137.5.10.163.in-addr.arpa. 86400 IN PTR mac137.info.unlp.edu.ar.  
161.5.10.163.in-addr.arpa. 86400 IN PTR sherlock.info.unlp.edu.ar.
```



# Enumeración - Netbios

```
nicolas@poseidon:~$ nbtscan 163.10.100/24
Doing NBT name scan for addresses from 163.10.100/24
```

IP address	NetBIOS Name	Server	User	MAC address
163.10.100.1	WSUS-UNLP	<server>	<unknown>	00:0c:29:09:96:77
163.10.100.2	Sendto failed: Permission denied			
163.10.100.3	EUROPA	<server>	<unknown>	00:15:c5:32:f5:04
163.10.100.4	SERVIDORLIVIANO	<server>	SERVIDORLIVIANO	00:00:00:00:00:00
163.10.100.5	PEPE	<server>	<unknown>	00:0b:6a:cd:12:59
163.10.100.6	LINTIDC	<server>	LINTIDC	00:00:00:00:00:00
163.10.100.7	NEPTUNO	<server>	NEPTUNO	00:00:00:00:00:00
163.10.100.8	LIHUEN-008BF8	<server>	LIHUEN-008BF8	00:00:00:00:00:00
163.10.100.9	Sendto failed: Permission denied			
163.10.100.10	2003LIVIANO	<server>	<unknown>	00:0c:29:e9:b1:6a
163.10.100.11	LIHUEN-E87C98	<server>	LIHUEN-E87C98	00:00:00:00:00:00
163.10.100.12	A1	<server>	<unknown>	00:0a:e6:cd:cc:ac
163.10.100.13	DEBIAN	<server>	DEBIAN	00:00:00:00:00:00
163.10.100.14	CMP-E75F0890AE5	<server>	<unknown>	00:13:8f:a7:35:e8
163.10.100.15	DEBIANII	<server>	DEBIANII	00:00:00:00:00:00

```
nicolas@poseidon:~$ smbclient -U nmacia -L NEPTUNO
Password:
Domain=[REDES] OS=[Unix] Server=[Samba 3.0.24]
```

Sharename	Type	Comment
IPC\$	IPC	IPC Service (neptuno server)
print\$	Disk	Printer Drivers
Voluntariado	Printer	Voluntariado
hp	Printer	hp

```
Domain=[REDES] OS=[Unix] Server=[Samba 3.0.24]
```

Server	Comment
LINTIDC	lintidc
NEPTUNO	neptuno server

Workgroup	Master
REDES	LINTIDC





# Fingerprinting

## OS Fingerprinting

Este proceso permite determinar la identidad del sistema operativo del host remoto, analizando los paquetes que provienen del mismo. Permite identificar: impresoras, routers, access points, centrales telefonicas, desktops windows, servidores UNIXs

Existen distintas técnicas que se basan en cómo responde el host objetivo a los mensajes ICMP o TCP.

<http://nmap.org/book/osdetect.html>

## Service Fingerprinting

Este proceso permite determinar para un servicio dado, el protocolo, el servidor y la versión, en base a las respuestas recibidas.



# Fingerprinting - httpprint

Si se puede hacer banner grabbing es más fácil

```
$ nc 202.41.76.251 80  
HEAD / HTTP/1.0
```

From an Apache 1.3.23 server:

```
HTTP/1.1 200 OK  
Date: Sun, 15 Jun 2003 17:10:49 GMT  
Server: Apache/1.3.23  
Last-Modified: Thu, 27 Feb 2003 03:48:19 GMT  
ETag: "32417-c4-3e5d8a83"  
Accept-Ranges: bytes  
Content-Length: 196  
Connection: close  
Content-Type: text/html
```

```
$ nc 202.41.76.251 80  
HEAD / HTTP/1.0
```

From a Microsoft IIS 5.0 server:

```
HTTP/1.1 200 OK  
Server: Microsoft-IIS/5.0  
Expires: Tue, 17 Jun 2003 01:41:33 GMT  
Date: Mon, 16 Jun 2003 01:41:33 GMT  
Content-Type: text/html  
Accept-Ranges: bytes  
Last-Modified: Wed, 28 May 2003 15:32:21 GMT  
ETag: "b0aac0542e25c31:89d"  
Content-Length: 7369
```

```
$ nc 202.41.76.251 80  
HEAD / HTTP/1.0
```

From a Netscape Enterprise 4.1 server:

```
HTTP/1.1 200 OK  
Server: Netscape-Enterprise/4.1  
Date: Mon, 16 Jun 2003 06:19:04 GMT  
Content-type: text/html  
Last-modified: Wed, 31 Jul 2002 15:37:56 GMT  
Content-length: 57  
Accept-ranges: bytes  
Connection: close
```



# Fingerprinting - httpprint

Sino, se puede deducir a partir del ordenamiento de los headers

## Response from Apache 1.3.23

```
$ nc apache.example.com 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Sun, 15 Jun 2003 17:10:49 GMT
Server: Apache/1.3.23
Last-Modified: Thu, 27 Feb 2003 03:48:19 GMT
ETag: "32417-c4-3e5d8a83"
Accept-Ranges: bytes
Content-Length: 196
Connection: close
Content-Type: text/html
```

## Response from IIS 5.0



```
$ nc iis.example.com 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Content-Location: http://iis.example.com/Default.htm
Date: Fri, 01 Jan 1999 20:13:52 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Fri, 01 Jan 1999 20:13:52 GMT
ETag: W/"e0d362a4c335be1:ae1"
Content-Length: 133
```

## Response from Netscape Enterprise 4.1

```
$ nc netscape.example.com 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Server: Netscape-Enterprise/4.1
Date: Mon, 16 Jun 2003 06:01:40 GMT
Content-type: text/html
Last-modified: Wed, 31 Jul 2002 15:37:56 GMT
Content-length: 57
Accept-ranges: bytes
Connection: close
```

httpprint web server fingerprinting report						
host	port	ssl	banner reported	banner deduced	icon	confidence
192.168.253.132	80		Microsoft-IIS/6.0	Microsoft-IIS/6.0		
SSL analysis						
httpprint © 2003-2005 net-square						

[http://www.net-square.com/httpprint/httpprint\\_paper.html](http://www.net-square.com/httpprint/httpprint_paper.html)



# Escaneo de puertos

El objetivo es determinar qué puertos están abiertos en un host o servidor determinado.

Si el puerto está abierto, eso implica que hay un proceso atendiendo a los requerimientos que llegan al puerto.

El proceso es software el cual puede estar desactualizado, por lo que puede tener vulnerabilidades que afecten su normal funcionamiento o la seguridad del sistema y sus datos.







# Técnicas de port scanning

## Técnicas de scanning - TCP:

### Open TCP scanning:

*TCP Connect() Scanning (Vanilla connect scanning)*

### Stealth TCP scanning

*Half-open SYN flag scanning*

*Inverse TCP flag scanning*

*ACK flag probe scanning*

### Third-party and spoofed TCP scanning

*TCP Idle Scanning (IP ID header scanning)*

*FTP bounce scanning*

*Proxy bounce scanning*

*Sniffer-based spoofed scanning*

## Técnicas de scanning - UDP:

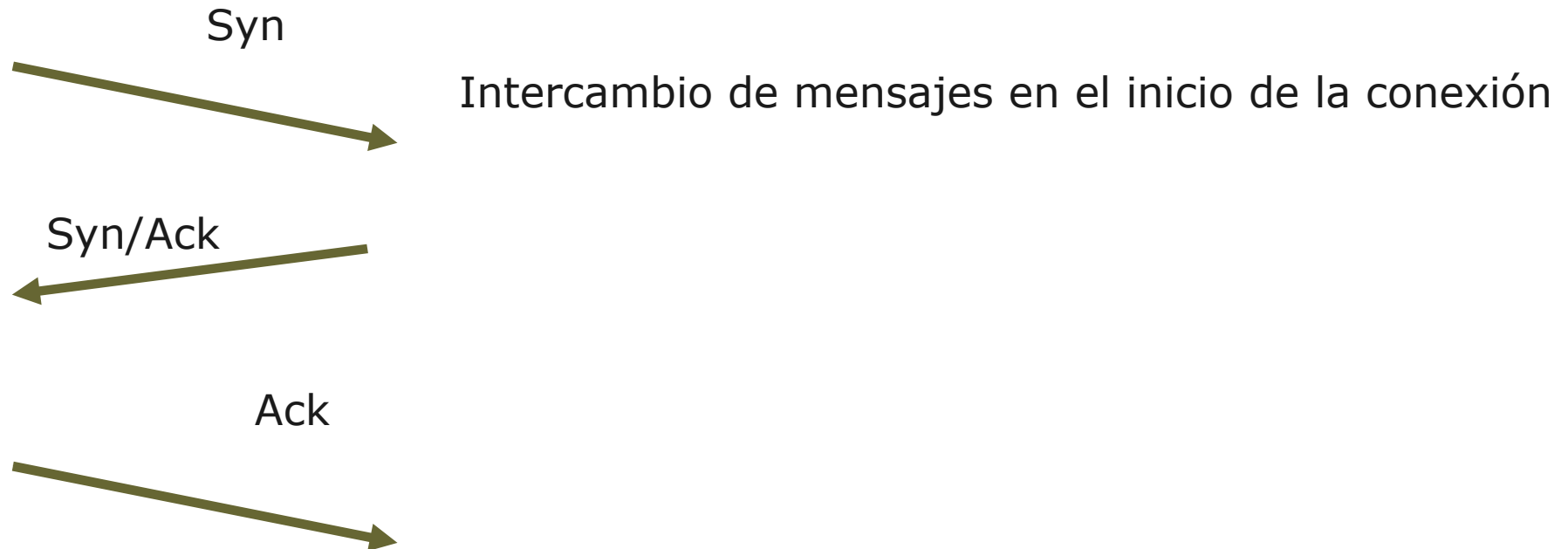
### UDP ICMP port unreachable scanning



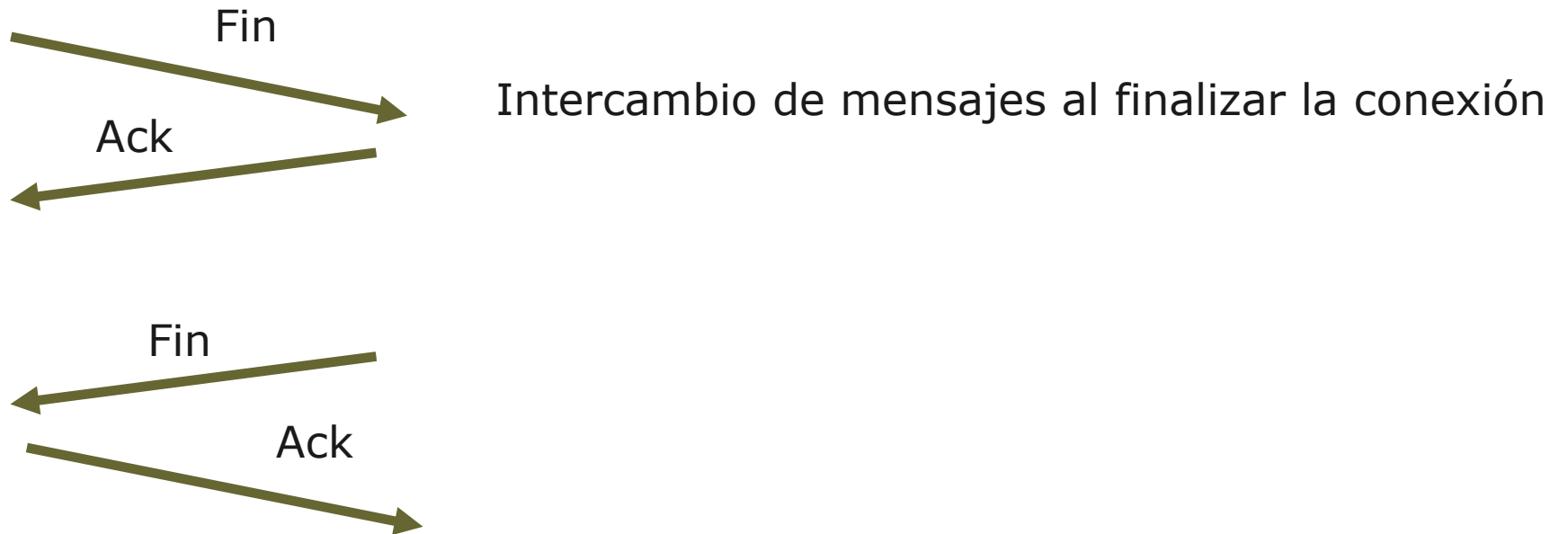


# Sesiones TCP – Inicio de conexión

## *Saludo de tres vías*

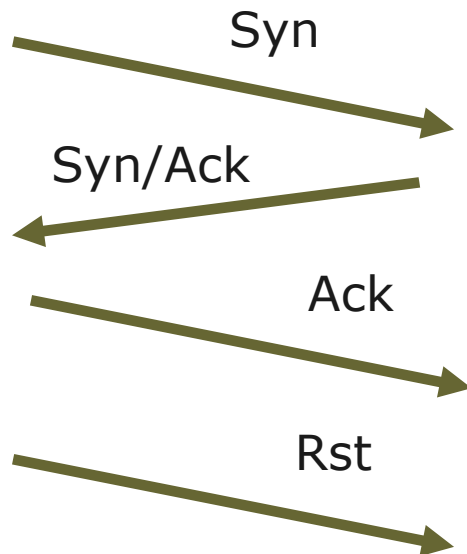


# Sesiones TCP – Cierre de conexión

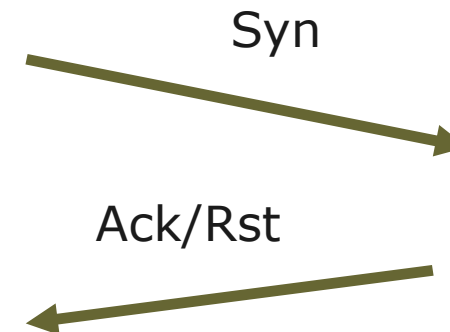


# *TCP Connect() Scanning*

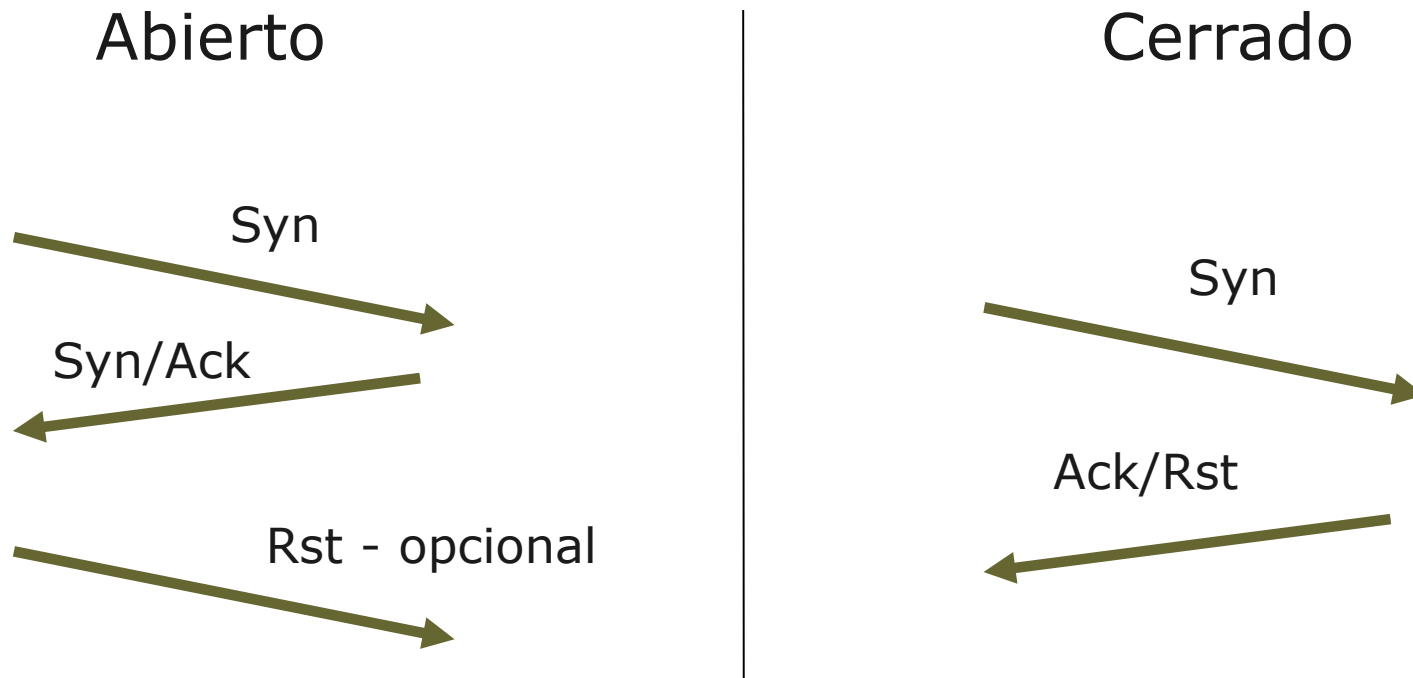
Abierto



Cerrado



# *Half-open SYN flag scanning*



# *Inverse TCP flag scanning*

## Abierto

Probe packet (FIN/URG/PSH, SYN/ACK, NULL, XMAS)



No hay respuesta



## Cerrado

Probe packet (FIN/URG/PSH, SYN/ACK, NULL, XMAS)

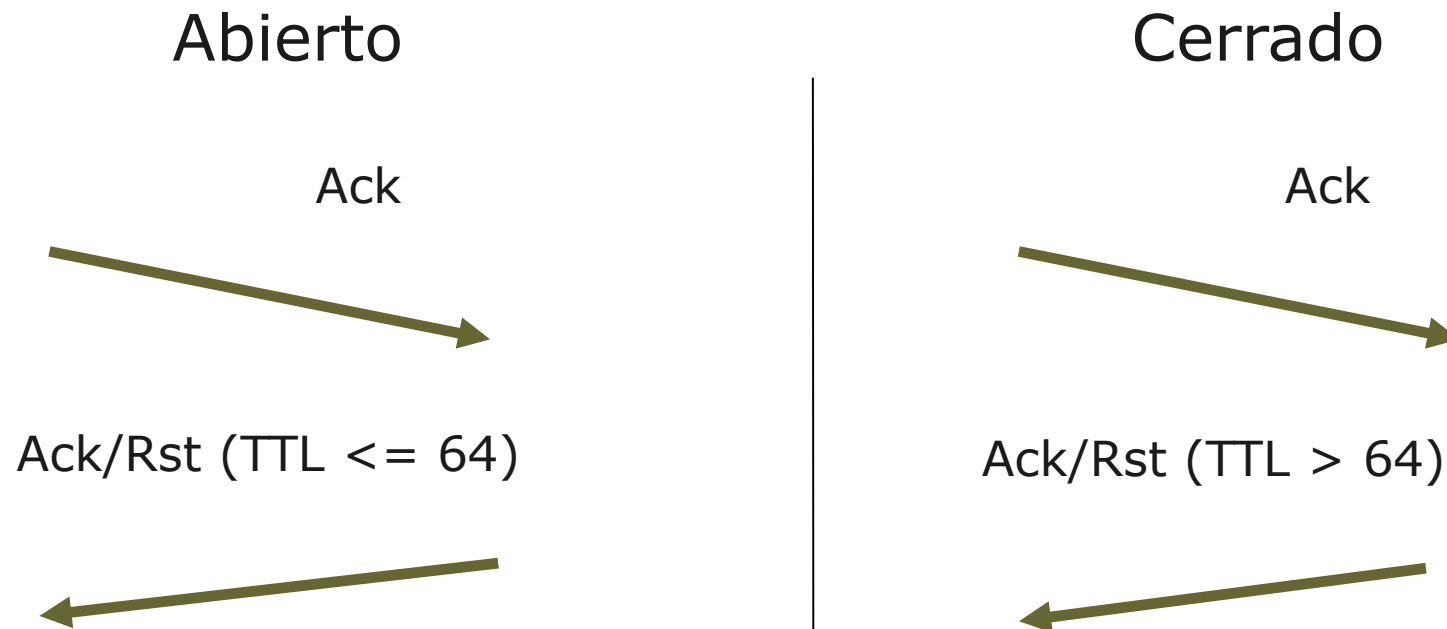


Ack/Rst



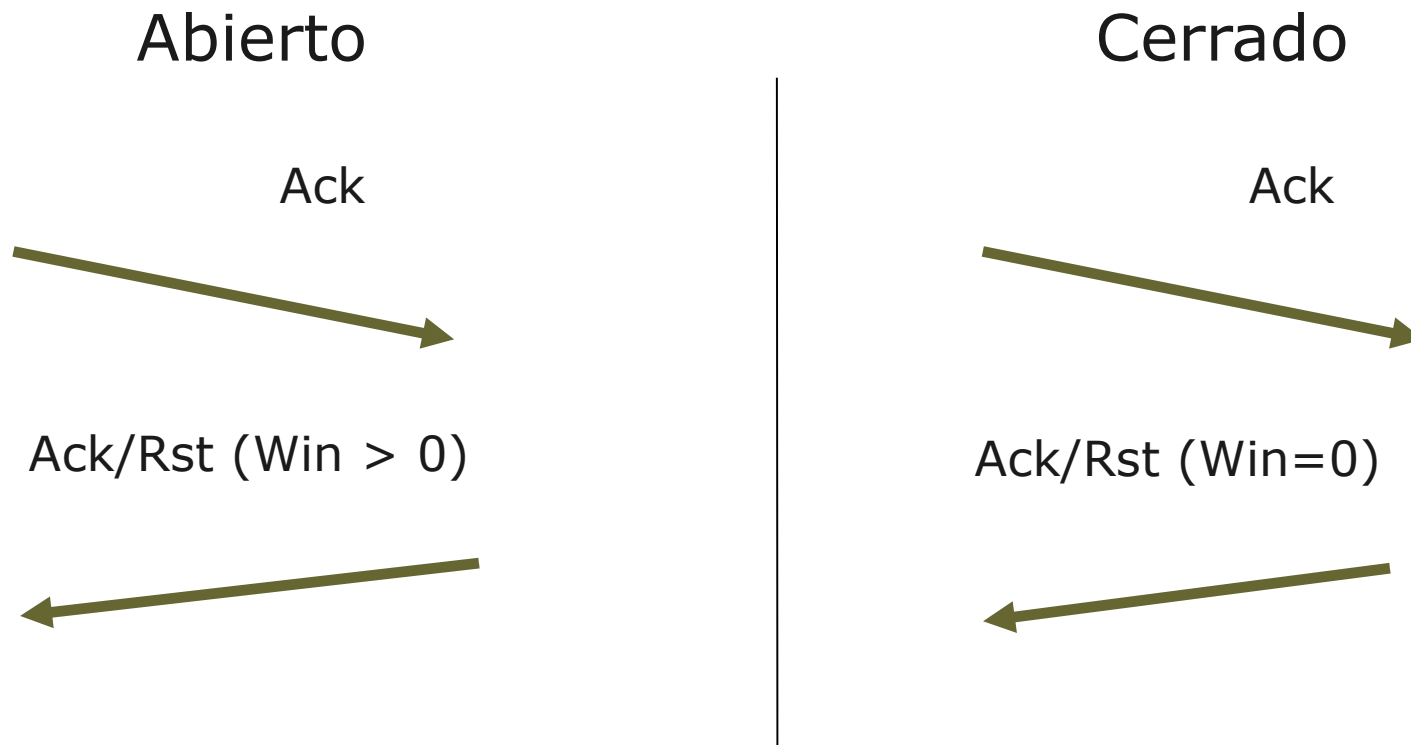
# *Ack flag probe scanning*

## **Análisis del campo TTL de los paquetes recibidos**



# *Ack flag probe scanning*

## **Análisis del campo Window de los paquetes recibidos**



# TCP idle scan

Esta técnica permite al atacante realizar el escaneo sin que pueda quedar registrado ningún paquete proveniente desde su dirección IP.

En este escaneo, se distinguen los siguientes actores:

- Atacante: quien va a realizar el escaneo
- Víctima: quien va a recibir el escaneo
- Zombie: máquina en nombre de la cual se va a realizar el escaneo.





# TCP idle scan - Zombie

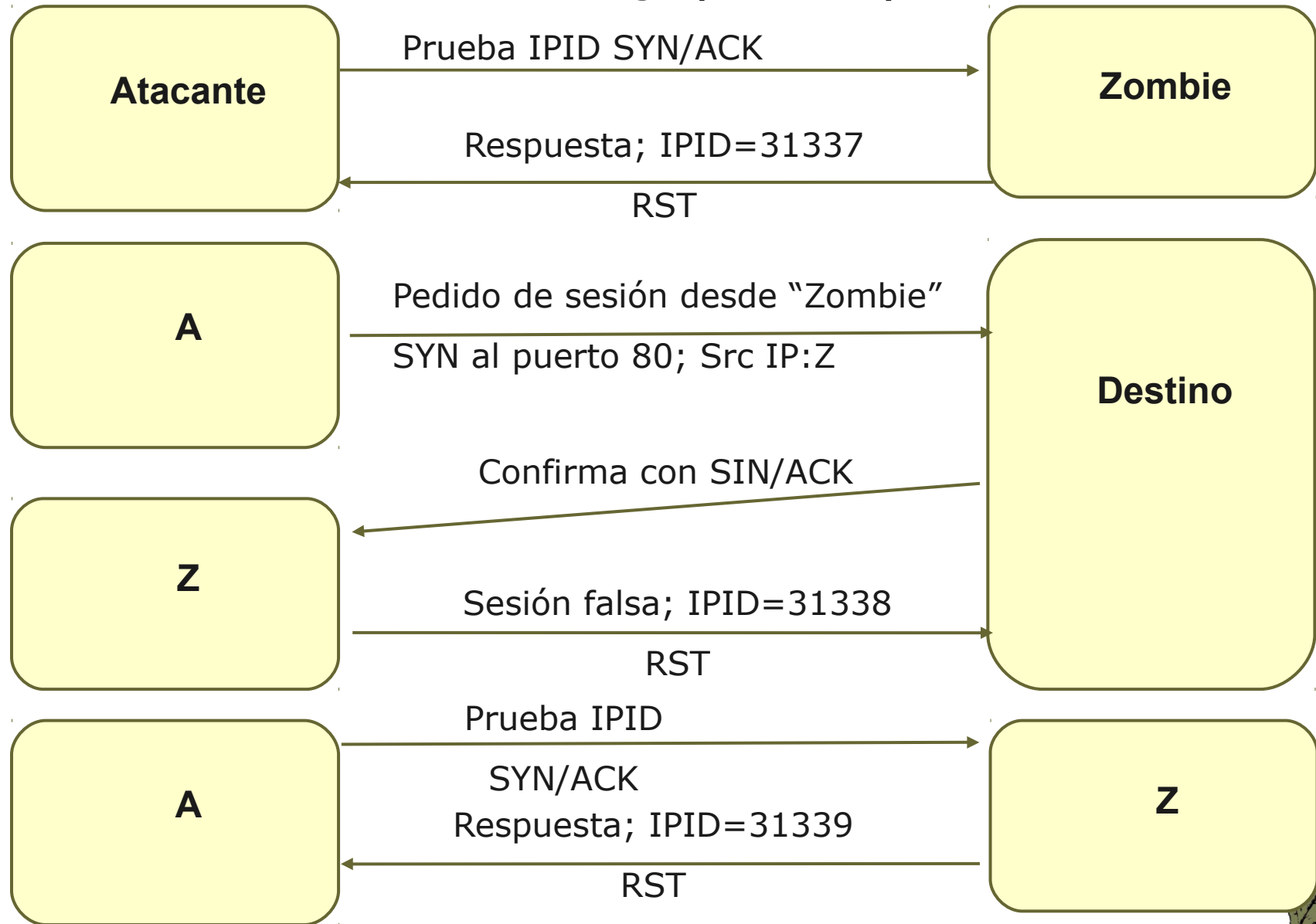
Para que el zombie sirva a nuestro propósito, el mismo debe cumplir con los siguientes requisitos:

- Debe tener poco tráfico
- Debe ser predecible el valor del campo IP ID de los paquetes que éste envía

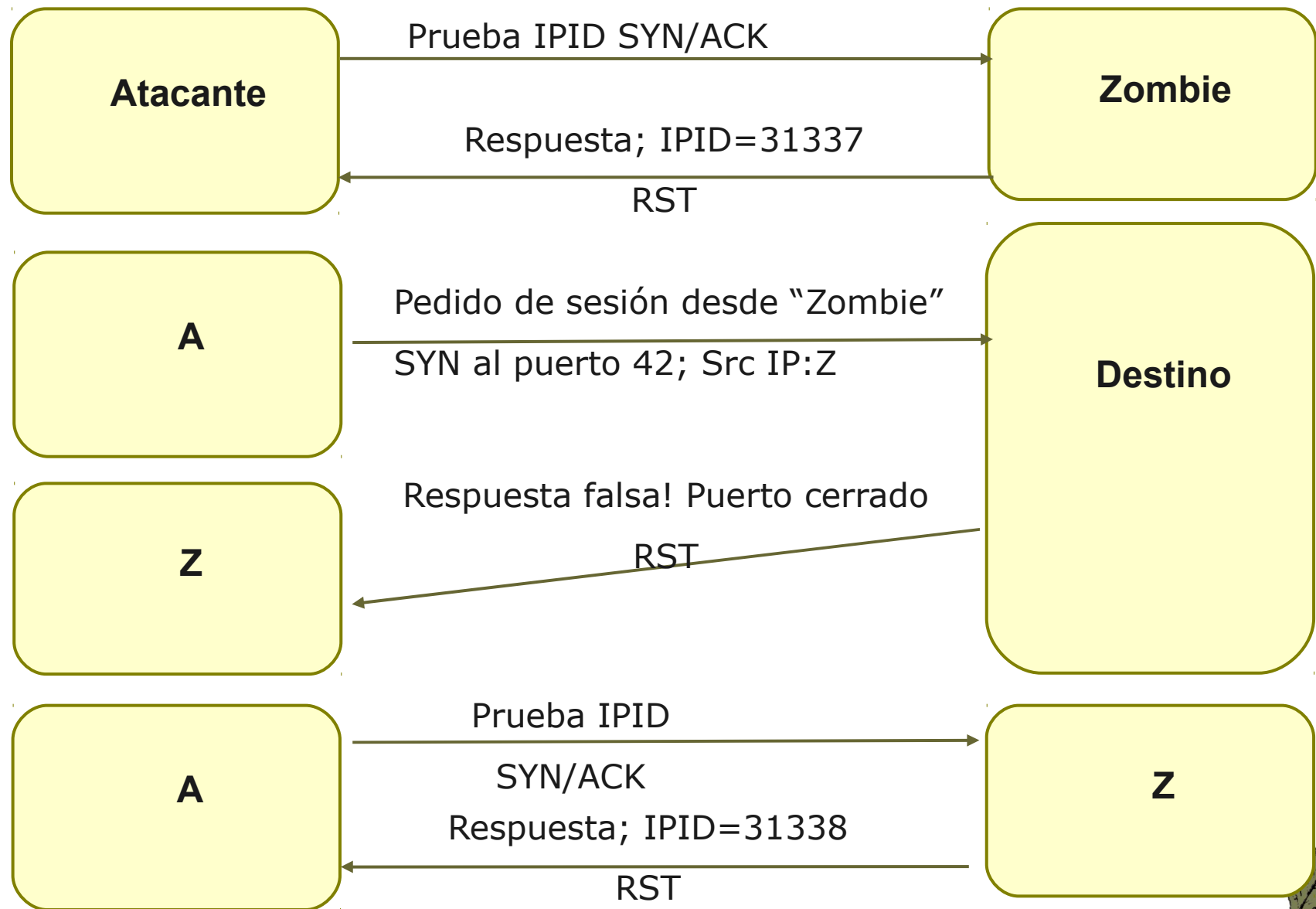
```
nico@yoko:~$ sudo hping3 -S -p 80 -S 192.168.70.122
HPING 192.168.70.122 (wlan0 192.168.70.122): S set, 40 headers + 0 data bytes
len=46 ip=192.168.70.122 ttl=128 id=7311 sport=80 flags=RA seq=0 win=0 rtt=1.8 ms
len=46 ip=192.168.70.122 ttl=128 id=7312 sport=80 flags=RA seq=1 win=0 rtt=1.7 ms
len=46 ip=192.168.70.122 ttl=128 id=7313 sport=80 flags=RA seq=2 win=0 rtt=1.6 ms
len=46 ip=192.168.70.122 ttl=128 id=7314 sport=80 flags=RA seq=3 win=0 rtt=1.8 ms
len=46 ip=192.168.70.122 ttl=128 id=7315 sport=80 flags=RA seq=4 win=0 rtt=1.4 ms
len=46 ip=192.168.70.122 ttl=128 id=7316 sport=80 flags=RA seq=5 win=0 rtt=1.4 ms
len=46 ip=192.168.70.122 ttl=128 id=7317 sport=80 flags=RA seq=6 win=0 rtt=1.4 ms
```



# TCP Idle Scanning (Cont.)

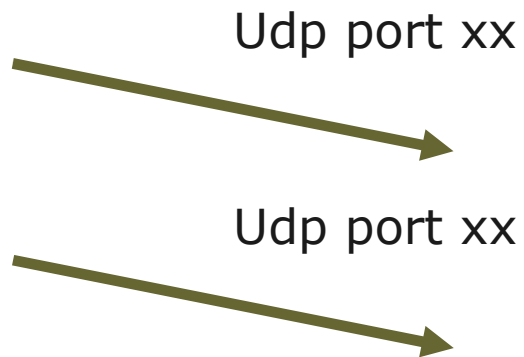


# TCP Idle Scanning (Cont.)

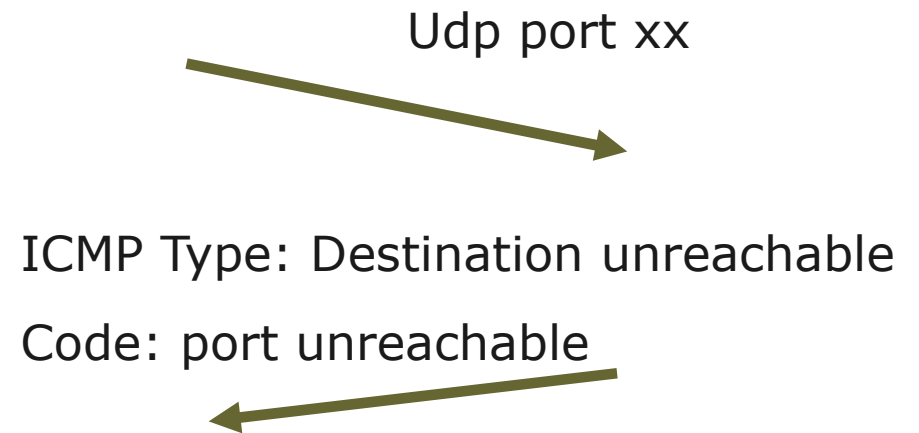


# *UDP ICMP port unreachable scanning*

Abierto



Cerrado



# Escaneadores de vulnerabilidades

Además de implementar la funcionalidad de un escaner de puertos, va un poco más lejos.

- Escanean los puertos del host testeado
- Determinan la aplicación que está brindando el servicio descubierto.
- Intentan determinar la versión de la aplicación.
- Determinan si las aplicaciones descubiertas tienen vulnerabilidades conocidas. Para ésto contrastan lo encontrado con una base de datos que se debe actualizar periódicamente.



# Escaneadores de vulnerabilidades- Ejemplos

Languad: [<http://www.gfi.com/lannetscan/>] Producto comercial para Windows

Nessus: [<http://www.nessus.org/nessus/>] Paso a ser comercial recientemente

Retina [<http://www.eeye.com/Retina/>] Producto comercial para Windows

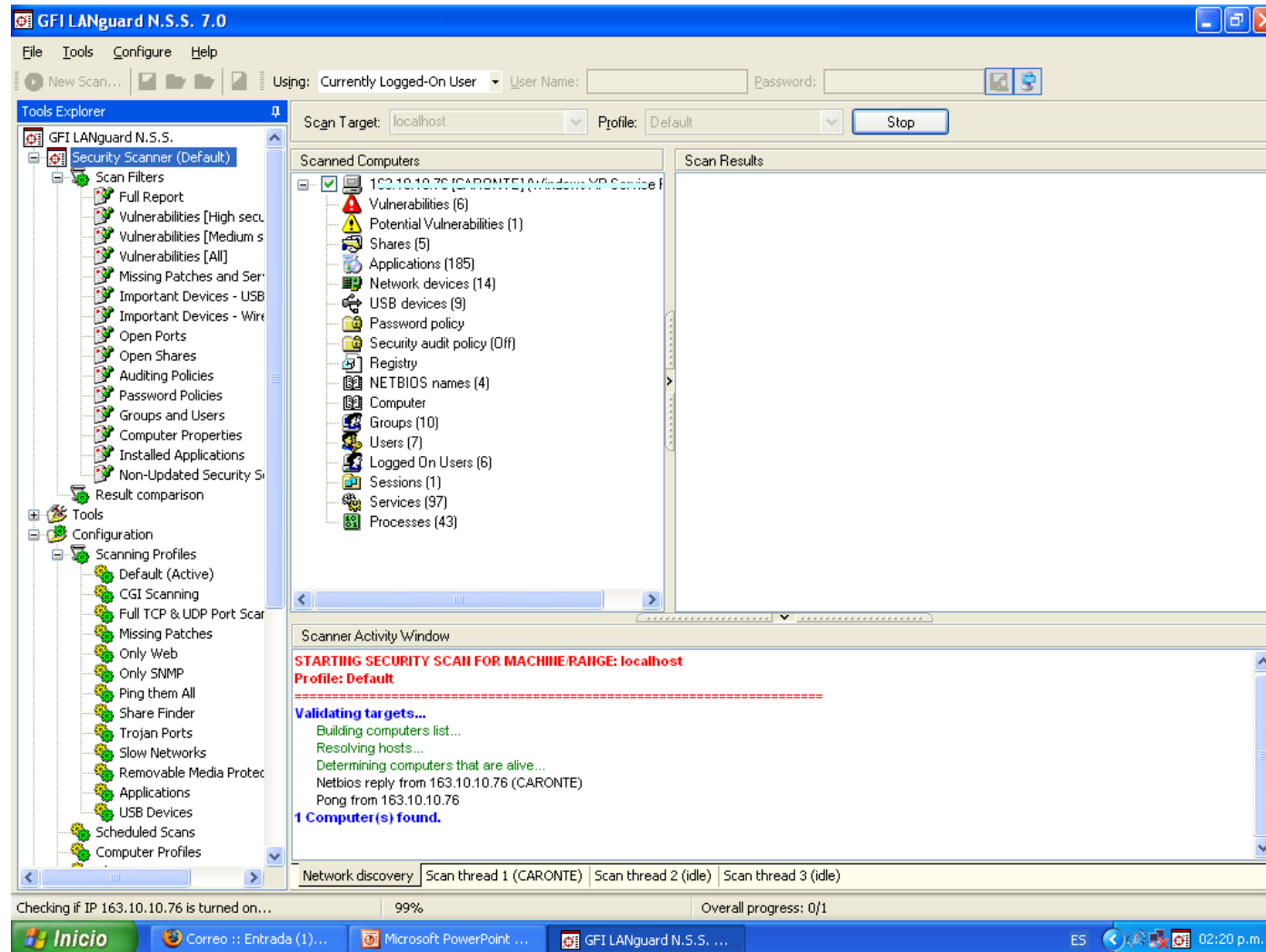
Saint [<http://www.saintcorporation.com/>] Producto comercial

OpenVAS [<http://www.openvas.org/>] Es un fork open-source de Nessus

Nikto: [<http://www.cirt.net/code/nikto.shtml>] Web Server Scan



# Escaneadores de puertos y vulnerabilidades- LANGUARD



<http://www.gfi.com/lannetscan/>





# Nessus

Es un scanner de vulnerabilidades que cuenta con una arquitectura cliente/servidor cuyos componentes son:

El servidor Nessus, que ejecuta el escaneo

El cliente Nessus que presenta los resultados al usuario.

Los plugins Nessus

La base de datos de conocimiento Nessus.

Los resultados los presenta en reportes con distintos formatos: texto plano, XML, HTML y LaTeX

Provee funcionalidad adicional para testear el nivel de vulnerabilidad de la red (como por ej. Ejecutar auditoría de passwords usando métodos de diccionario o ataques de fuerza bruta)

Desde el 31 de julio de 2008 se volvió comercial

<http://www.nessus.org/nessus/>







OPENVAS (Open Vulnerability Assessment System) es distribuido bajo licencia GNU GPL

Deriva de Nessus que es un producto propietario en el año 2008.

**OpenVAS-Server:** Es el núcleo de OpenVAS

**OpenVAS-Libraries:** Librerías que contienen funcionalidad que es utilizada por el OpenVAS – Server.

**OpenVAS-LibNASL:** Este módulo contiene la funcionalidad requerida para que el OpenVAS-Server interactúe con NASL (Nessus Attack Scripting Language).

**OpenVAS-Plugins:** Contiene la base de datos de las NVTs (Network Vulnerability Tests). Debe ser actualizada con frecuencia.

**OpenVAS-Client:** El cliente se conecta con el OpenVAS-Server, procesa los resultados de los escaneos y los muestra al usuario

<http://www.openvas.org/>



# Escaner de propósito específico: Nikto

Es un scanner de vulnerabilidades de servidores WEB opensource (GPL).

Está orientado a examinar servidores Web para descubrir:

Configuraciones no adecuadas

Archivos y scripts por defecto

Archivos y scripts con problemas de seguridad

Software desactualizado

<http://www.cirt.net/code/nikto.shtml>



# Resultados de los análisis: Códigos

**CVE** = Common Vulnerabilities and Exposures: Son identificadores únicos para vulnerabilidades de seguridad publicamente conocidas.

Ej: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0222>

**CAN** = Vulnerabilidades candidatas a convertirse en CVE (discontinuado desde 2005)

Ej: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0649>

**BID** = Bugtraq ID: Son los IDs que asignan en Security Focus para las vulnerabilidades

<http://www.securityfocus.com/bid/17106>



# Resultados de los análisis: Códigos

Dependiendo del origen del reporte, identificadores de distintos orígenes que generalmente mapean con un CVE o un CAN:

## Ejemplos:

**USN-432-1** Ubuntu Security Notice **USN-432-1** que se corresponde con el **CVE-2007-1263**

**MDKSA-2007:055** Mandriva Linux Security Advisory **MDKSA-2007:055** con el **CVE-2007-1246**

**MS07-008** Microsoft Security Bulletin **MS07-008** con el **CVE-2007-0214**



# Otras formas de obtener Información

Craqueo de claves:

Fuerza Bruta: combinando conjunto de caracteres.

Diccionario: utilizando listas de palabras. Ej: megadic (2,2 GigaBytes)

Ejemplos:

Brutus

John the ripper

Cain y Abel



# Más referencias

“Network Security Assessment” – Chris McNab – O’Reilly

<http://www.insecure.org/>

<http://nmap.org/book/osdetect.html>

[http://net-square.com/httpprint/httpprint\\_paper.html](http://net-square.com/httpprint/httpprint_paper.html)

<http://packetstormsecurity.org/>

<http://www.securityfocus.com>

<http://www.cert.org/>

Back Track [http://www.remote-exploit.org/backtrack\\_download.html](http://www.remote-exploit.org/backtrack_download.html)

