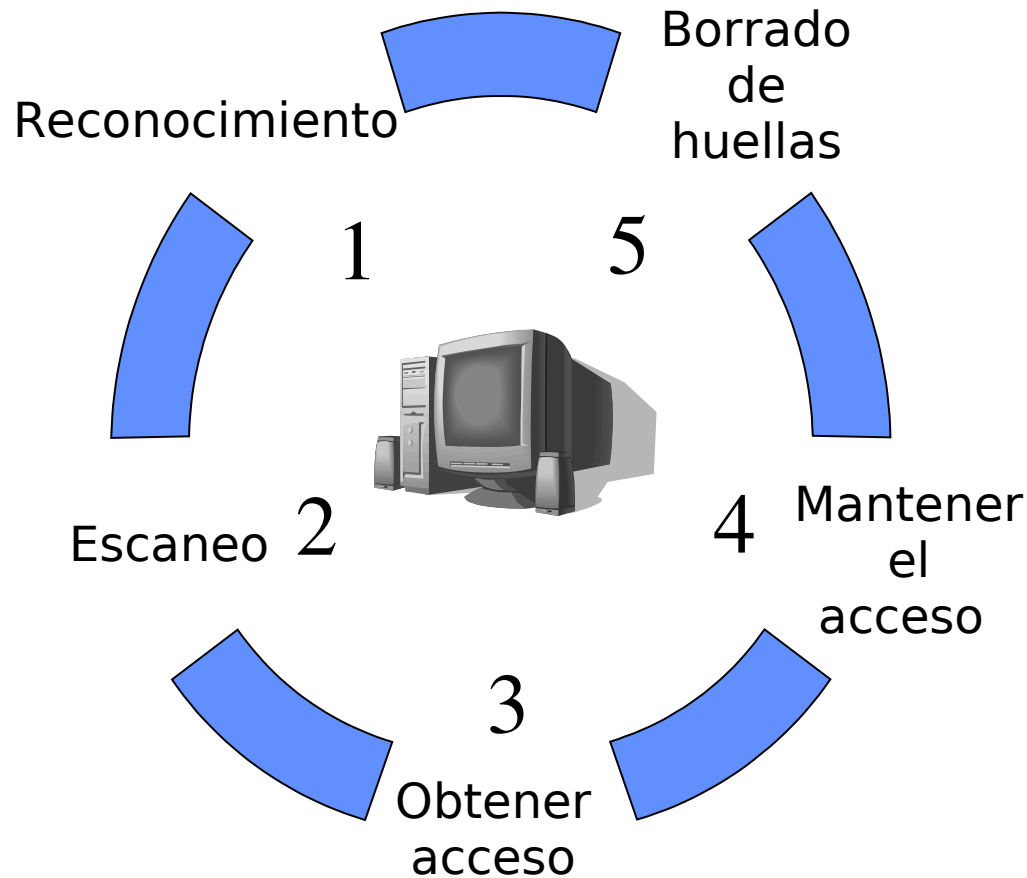


# Hacking Ético

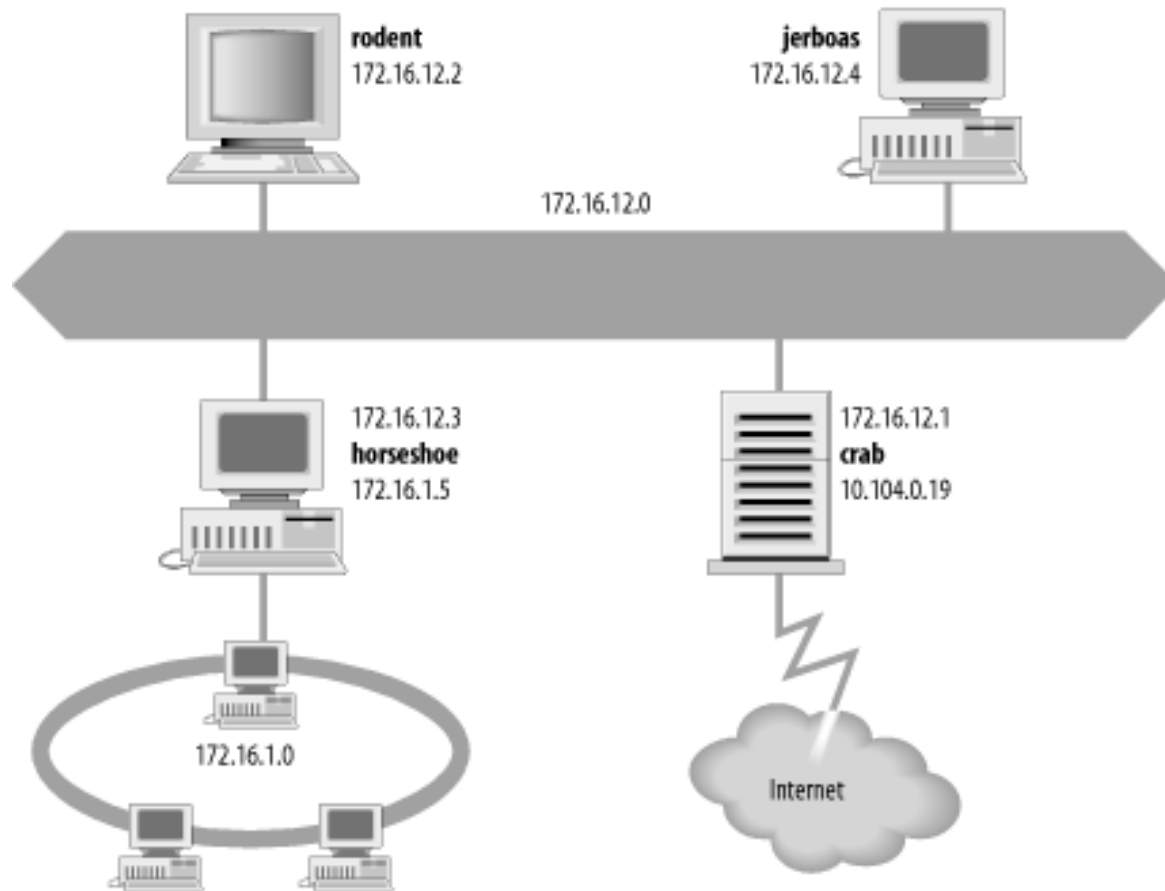
Módulo I

Fase 1: Obtención de  
información

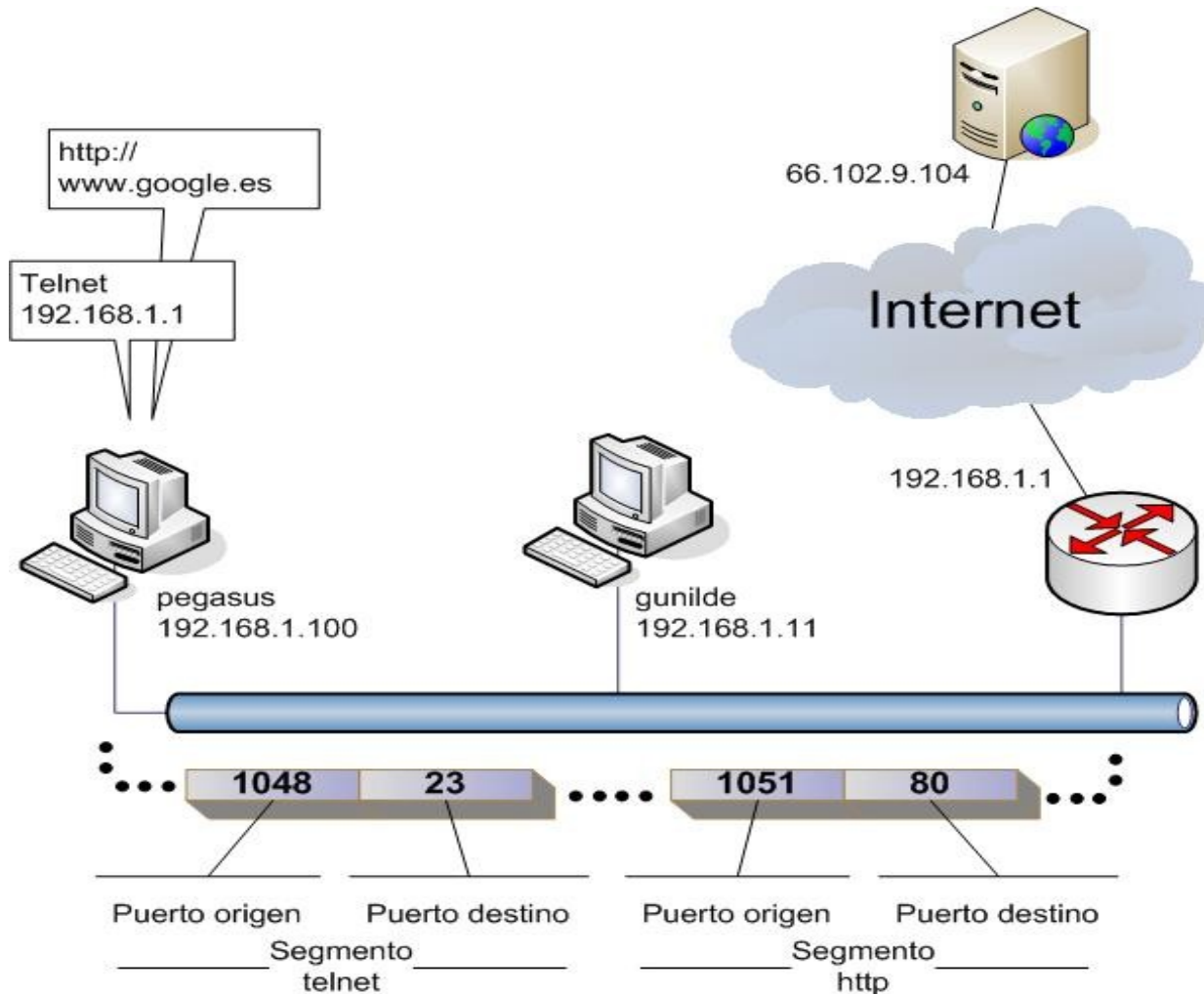
# Obtención de información



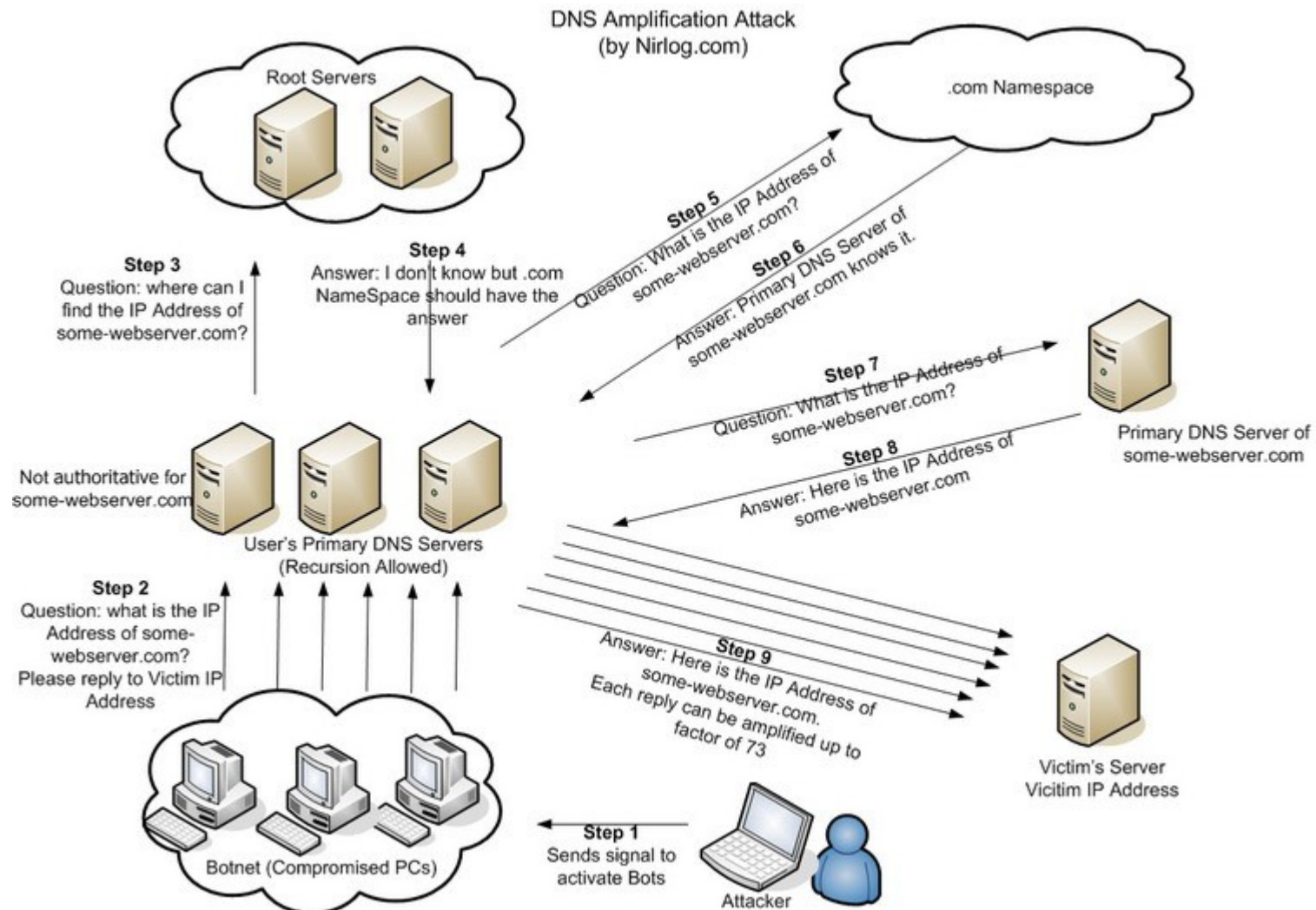
# Conceptos: TCP/IP



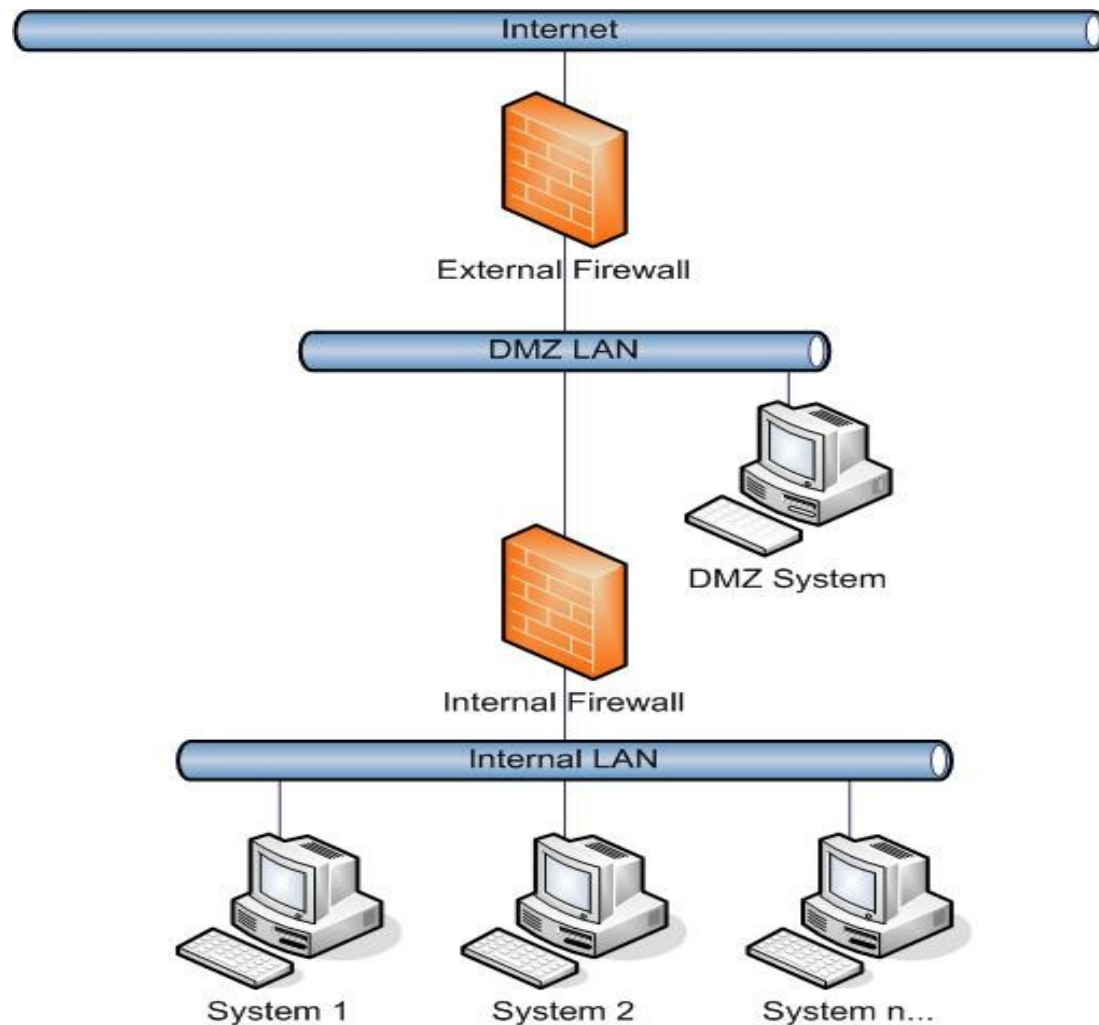
# Conceptos: Servicio y Puerto



# Conceptos: DNS



# Conceptos: DMZ



# Obtención de información

Dos fases en el pre-ataque:

- Obtención de información – Pasivo y legal
- Escaneo y Enumeración – Activo e ilegal (lo veremos después)

Metodología para la obtención de información de una empresa u organización.

Obtención de perfiles de seguridad de sus redes  
(Internet / Intranet / Extranet / Wireless)

# Obtener información inicial

## Incluiría:

- Nombres servidores DNS, algunas direcciones IP
- Localizaciones geográficas de la empresa.
- Contactos (Teléfono / mail)

## Fuentes de Información:

- Infojobs / monster
- Google hacking.
- Web de la empresa
- whois
- nslookup
- [www.all-nettols.com](http://www.all-nettols.com)



# Google hacking

“Google Hacking” es la acción de buscar en Google información sensible, generalmente con fines maliciosos.

- Productos vulnerables
- Ficheros que contienen claves
- Ficheros que contienen nombres de usuario
- Páginas con formularios de acceso
- Páginas que contienen datos relativos a vulnerabilidades
- Dispositivos hardware online

# Google hacking

Google   [Búsqueda avanzada](#)

Buscar en la Web  Buscar sólo páginas en español

---

Web [Mostrar opciones...](#) Resultados 1 - 10 de aproximadamente 1,950 de filetype:conf inurl:proftpd.conf -sample. (0.19 segundos)

[This is a basic ProFTPD configuration file \(rename it to ...](#)  
Formato de archivo: Desconocido - [Versión en HTML](#)  
# This is a basic ProFTPD configuration file (rename it to, # 'proftpd.conf' for actual use. It establishes a single server. # and a single anonymous login. ...  
[sdn.vlsm.org/share/Debian-Doc/manuals/debian-reference/.../proftpd.conf](http://sdn.vlsm.org/share/Debian-Doc/manuals/debian-reference/.../proftpd.conf) -

[/trunk/configs/ubuntu/proftpd/proftpd.conf - ispCP Omega | ISP ...](#) - [ [Traducir esta página](#) ]  
Revision 2505, 7.8 KB (checked in by nuxwin, 8 days ago). Re-integration of the branch nxw-cbc in the current development branch : Command used: ...  
[isp-control.net/ispcp/browser/trunk/.../proftpd.conf](http://isp-control.net/ispcp/browser/trunk/.../proftpd.conf) - [En caché](#) - [Similares](#) -

Google   [Advanced Search](#)

---

Web [Show options...](#) Results 1 - 3 of 3 for intitle:"Mail Server CMailServer Webmail" \*5.2". (0.09 seconds)

[Mail Server CMailServer WebMail 5.2.1](#)  
New User?Sign Up Now! Username Password Save account and password. This mail server powered by Youngzsoft.  
[web.u4x.net/mail/](http://web.u4x.net/mail/) - [Cached](#) - [Similar](#) -

[Mail Server CMailServer WebMail 5.2.1](#)  
Sign up here. Username\*. Password\*. Confirm New Password\*. Your Name. Comment. Contact email. This mail server powered by Youngzsoft.  
[web.u4x.net/mail/signup.asp](http://web.u4x.net/mail/signup.asp) - [Cached](#) - [Similar](#) -

Sponsored Links

[Complete Mail Server](#)  
Easy to install. Integrated Webmail  
Fast. Stops spam and viruses  
[netwinsite.com/surgemail.htm](http://netwinsite.com/surgemail.htm)

[See your ad here »](#)

# Fase 1 (pre ataque)- *Footprinting*

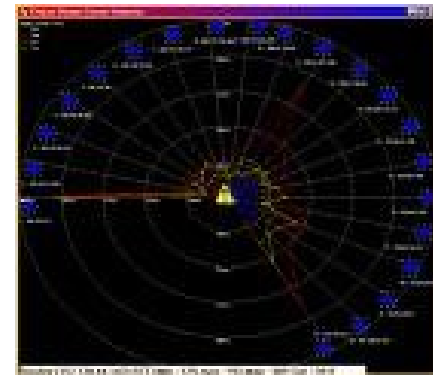
Obtener información inicial:

- whois
- nslookup

***InterNIC***

Localizar el rango de red:

- traceroute



# Whois

## Registrant:

targetcompany (targetcompany-DOM)  
XXX Everest Blk A.Enclave  
Ameerpet  
Hyderabad  
Andrapradesh, 500038  
IN  
Domain Name: targetcompany.COM

## Registrant:

targetcompany (targetcompany-DOM)  
# Street Address  
City, Province  
State, Pin, Country  
**Domain Name: targetcompany.COM**

## Administrative Contact:

R\*\*\*\*, J\*\*\*\* (RJXX2-ORG) targetcompany@HD1.VSML.NET.IN  
targetcompany  
XXX, Everest Block, A.Enclave,  
Ameerpet  
Hyderabad, Andrapradesh 500038  
IN 91 40 XXXX 329X Fax- 91 40 XXXX 329X

## Technical Contact:

S\*\*\*\*\*, V\*\*\*\* (VSXX) techcontact@WEBINDIA.COM  
XXS Inc  
XXX R Lane  
Hoffman Estates, IL 60194  
US. 408/XXX-XXXX 408/XXX-XXXX  
Record expires on 14-Oct-200X.  
Record created on 13-Oct-1997.  
Database last updated on 17-Mar-2003 07:49:04 EST.

## Administrative Contact:

Surname, Name (SNIDNo-ORG) targetcompany@domain.com  
targetcompany (targetcompany-DOM) # Street Address  
City, Province, State, Pin, Country  
Telephone: XXXXX Fax XXXXX

## Technical Contact:

Surname, Name (SNIDNo-ORG) targetcompany@domain.com  
targetcompany (targetcompany-DOM) # Street Address  
City, Province, State, Pin, Country  
Telephone: XXXXX Fax XXXXX

## Domain servers in listed order:

NS1.WEBINDIA.COM 204.XXX.140.X01  
NS2.WEBINDIA.COM 204.XXX.141.X01

## Domain servers in listed order:

NS1.WEBHOST.COM XXX.XXX.XXX.XXX  
NS2.WEBHOST.COM XXX.XXX.XXX.XXX

# Nslookup

```
jpancorb@localhost:~$
jpancorb@localhost:~$ nslookup
> set query=any
> osnius.com
Server:      80.58.61.250
Address:     80.58.61.250#53

Non-authoritative answer:
osnius.com   nameserver = dns1.peopleware.es.
osnius.com   nameserver = dns10.servidoresdns.net.
osnius.com   nameserver = dns2.peopleware.es.
osnius.com   nameserver = dns9.servidoresdns.net.

Authoritative answers can be found from:
dns10.servidoresdns.net internet address = 217.76.129.132
dns9.servidoresdns.net  internet address = 217.76.128.132
> server dns1.peopleware.es
Default server: dns1.peopleware.es
Address: 82.223.182.117#53
> osnius.com
Server:      dns1.peopleware.es
Address:     82.223.182.117#53

osnius.com
    origin = dns1.peopleware.es
    mail addr = hostmaster.peopleware.es
    serial = 2008070817
    refresh = 21600
    retry = 3600
    expire = 2419200
    minimum = 86400
osnius.com   nameserver = dns1.peopleware.es.
osnius.com   nameserver = dns2.peopleware.es.
Name:  osnius.com
Address: 217.76.130.141
osnius.com   mail exchanger = 10 smtp-01.servidoresdns.net.
> www.osnius.com
Server:      dns1.peopleware.es
Address:     82.223.182.117#53

Name:  www.osnius.com
Address: 217.76.130.141
> █
```

nslookup – resolución DNS  
(Sistema de Nombre de  
Dominios)

Con el nombre DNS de  
un equipo podemos  
obtener su ip.

Podemos obtener las ips  
de sus DNS internos.

Mediante sus DNS podemos  
obtener ips de sus máquinas  
web, de sus máquinas de mail,  
etc..

# Determinar el rango de red

## Incluiría:

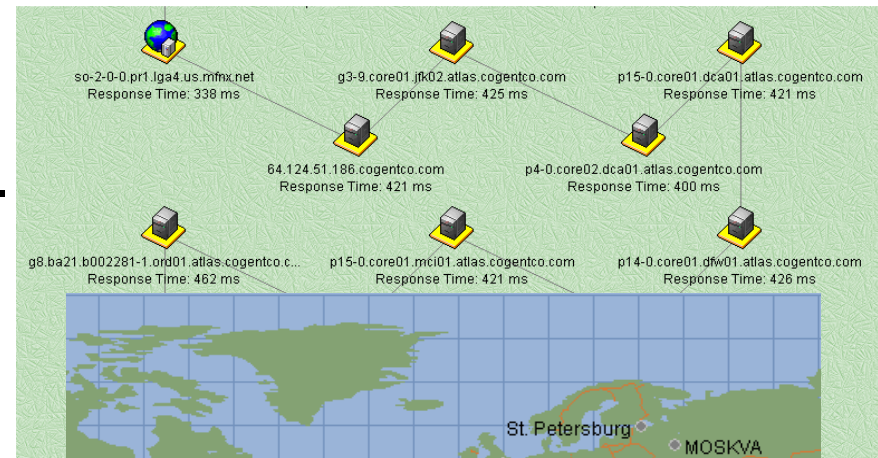
- Encontrar el rango de Ips.
- Encontrar la máscara de subred.
- Encontrar firewalls, DMZ, etc.

## Fuentes de información:

traceroute

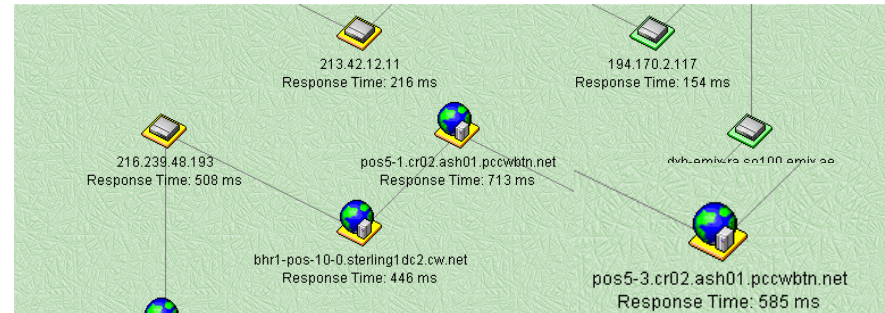
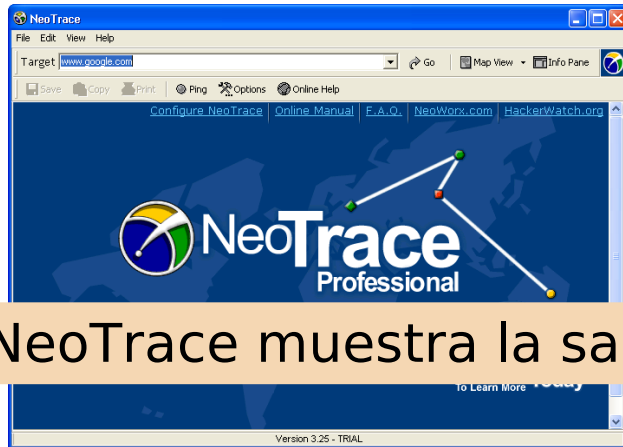
## Hacking Tool:

- NeoTrace / Geotrace.
- VisualRoute /Xroute (xt).
- Whatroute.

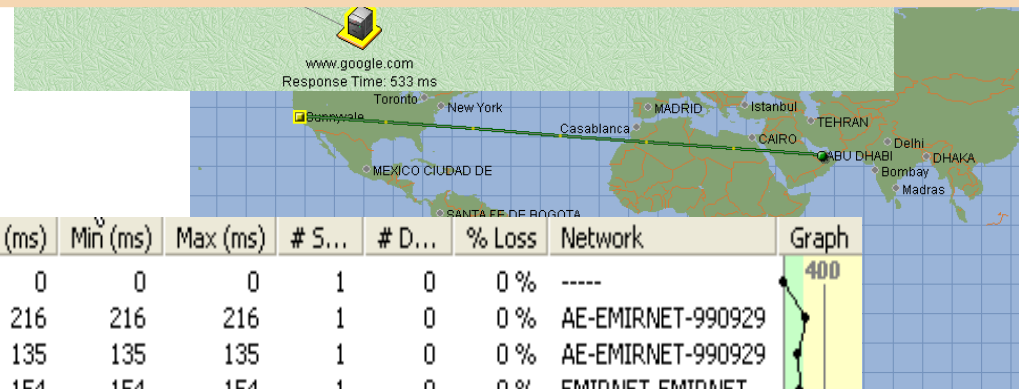


#	IP Address	Name	RT (ms)	Network	Graph
9	64.125.30.17	so-5-2-0.cr1.lga1.us.mfnx.net	339	ABOVENET	
10	208.185.0.246	so-0-0-0.cr1.lga2.us.mfnx.net	319	ABOVENET-6	
11	64.124.232.6	so-2-0-0.pr1.lga4.us.mfnx.net	338	ABOVENET	
12	64.124.51.186	64.124.51.186.cogentco.com	421	ABOVENET	
13	66.28.4.173	g3-9.core01.jfk02.atlas.cogentco.com	425	COGENT-NB-0000	
14	66.28.4.81	p4-0.core02.dca01.atlas.cogentco.com	400	COGENT-NB-0000	
15	66.28.4.21	p15-0.core01.dca01.atlas.cogentco.com	421	COGENT-NB-0000	
16	66.28.4.90	p14-0.core01.dfw01.atlas.cogentco.com	426	COGENT-NB-0000	
17	66.28.4.26	p15-0.core02.dfw01.atlas.cogentco.com	441	COGENT-NB-0000	
18	66.28.4.38	p15-0.core01.mci01.atlas.cogentco.com	421	COGENT-NB-0000	
19	66.28.4.34	p5-0.core02.ord01.atlas.cogentco.com	467	COGENT-NB-0000	
20	66.28.66.86	g8.ba21.b002281-1.ord01.atlas.cogentco.com	462	COGENT-NB-0000	

# Tool: NeoTrace (Now McAfee Visual Trace) – Geotrace (GNU)



NeoTrace muestra la salida de traceroute visualmente en un mapa.



#	IP Address	Name	RT (ms)	Ave (ms)	Min (ms)	Max (ms)	# S...	# D...	% Loss	Network	Graph
1	217.165.236.73	SAM	0	0	0	0	1	0	0 %	----	
2	213.42.12.11	----	216	216	216	216	1	0	0 %	AE-EMIRNET-990929	
3	213.42.12.130	----	135	135	135	135	1	0	0 %	AE-EMIRNET-990929	
4	194.170.2.117	----	154	154	154	154	1	0	0 %	EMIRNET-EMIRNET	
5	195.229.31.66	dxb-emix-rb.ge130.emix.ae	159	159	159	159	1	0	0 %	AE-EMIRNET-971125	
6	195.229.0.234	dxb-emix-ra.so100.emix.ae	139	139	139	139	1	0	0 %	EMIRNET-EMIRNET	
7	166.63.210.62	bcr2.thamesside.cw.net	442	442	442	442	1	0	0 %	CW-NETCS2	
8	63.216.0.42	pos5-1.cr02.ash01.pccwbtn.net	713	713	713	713	1	0	0 %	CAIS-CIDR7	
9	206.24.238.166	bhr1-pos-10-0.sterling1dc2.cw.net	446	446	446	446	1	0	0 %	CW-05BLK	
10	216.239.48.193	----	508	508	508	508	1	0	0 %	GOOGLE	
11	216.109.88.218	218-google-exodusdc.exodus.net	442	442	442	442	1	0	0 %	DC3-8	
12	216.239.39.99	www.google.com	533	533	533	533	1	0	0 %	GOOGLE	

# Tool: VisualRoute Mail Tracker

**Report for olympus.bic.nus.edu.sg [137.132.19.100]**

Analysis: 'olympus.bic.nus.edu.sg' was found in 24 hops (TTL=240). It is a SMTP server (ESMTP Sendmail 8.12.8/8.12.7).

eMailTracker by Visualware

tinwee@bic.nus.edu.sg

Server	Prio	IP Address	Status
olympus.bic.nus.edu.sg	10	137.132.19.100	ESMTP Sendmail 8.12.8/8.12.7

[Click on a server name to start a VisualRoute trace](#)

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		217.165.221.153	SAM	*			0	Emirates Internet
1		213.42.12.6	-	(United Arab Emirates)		2537		Emirates Telecommunicati
2		213.42.12.131	-	(United Arab Emirates)		2513		Emirates Telecommunicati
3		194.170.2.117	-	(United Arab Emirates)		2467		Emirates Internet
4		195.229.31.35	auh-emix-rb.ge6303.er	(United Arab Emirates)		2429		Emirates Telecommunicati
5		195.229.31.34	auh-emix-ra.ge6303.er	(United Arab Emirates)		2421		Emirates Telecommunicati
6		62.216.144.25	-	(United Kingdom)	*	2766		FLAG Telecom Limited
7		62.216.140.9	ge-1-0-0.0.core1.sfr1.fl	(United Kingdom)	*	2894		FLAG Telecom Limited
8		166.90.133.165	gige4-1-116.ipcolo2.Sa	San Francisco, CA, US	-08:00	2655		Level 3 Communications, It
9		209.244.14.201	gigabitethernet4-2.core	San Francisco, CA, US	-08:00	2695		Level 3 Communications, It
10		209.247.10.233	so-4-0-0.mp2.SanFran	San Francisco, CA, US	-08:00	3008		Level 3 Communications, It



# Ejemplo

wikipedia.org

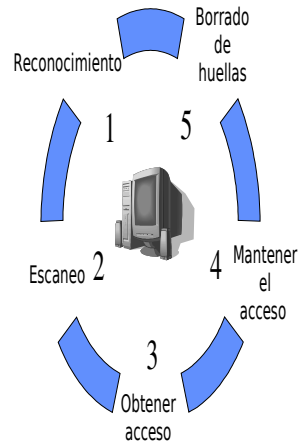
- whois - datos de la empresa. DNS de la empresa
- nslookup - sacar la IP de su servidor mail.
- traceroute - obtener la IP de su cortafuegos.

# Hacking Ético

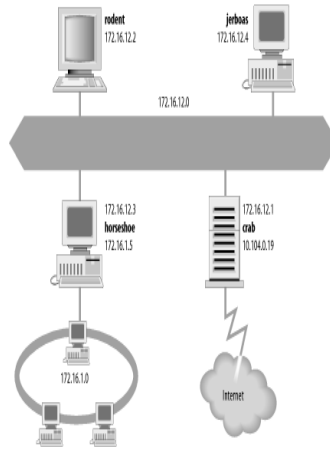
Módulo I

Fase 1: Obtención de  
información

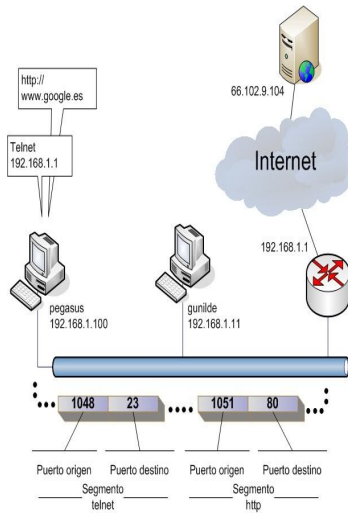
# Obtención de información



# Conceptos: TCP/IP



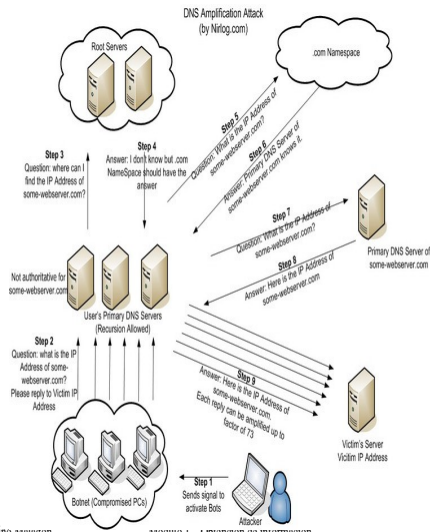
# Conceptos: Servicio y Puerto



Constantino Malagón  
Jesús Pancorbo

Módulo 1 – Obtención de información

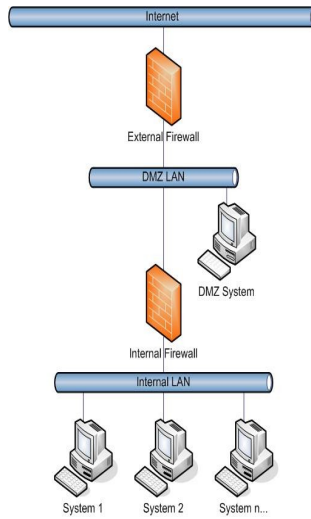
# Conceptos: DNS



Constantino Araagon  
Jesús Pancorbo

MODULO 1 - UTILIZACION DE INFORMACION

# Conceptos: DMZ



# Obtención de información

Dos fases en el pre-ataque:

- Obtención de información - Pasivo y legal
- Escaneo y Enumeración - Activo e ilegal (lo veremos después)

Metodología para la obtención de información de una empresa u organización.

Obtención de perfiles de seguridad de sus redes  
(Internet / Intranet / Extranet / Wireless)



## Obtener información inicial

### Incluiría:

- Nombres servidores DNS, algunas direcciones IP
- Localizaciones geográficas de la empresa.
- Contactos (Teléfono / mail)

### Fuentes de Información:

- Infojobs / monster
- Geogle hacking.
- Web de la empresa
- whois
- nslookup
- [www.all-nettols.com](http://www.all-nettols.com)

## Google hacking

“Google Hacking” es la acción de buscar en Google información sensible, generalmente con fines maliciosos.

- Productos vulnerables
- Ficheros que contienen claves
- Ficheros que contienen nombres de usuario
- Páginas con formularios de acceso
- Páginas que contienen datos relativos a vulnerabilidades
- Dispositivos hardware online

# Google hacking

Google filetype:conf inurl:proftpd.conf-sample  [Búsqueda avanzada](#)

Buscar en la Web  Buscar sólo páginas en español

Web [Mostrar opciones...](#) Resultados 1 - 10 de aproximadamente 1,950 de filetype:conf inurl:proftpd.conf-sample (0.19 segundos)

[This is a basic ProFTPD configuration file \(rename it to ...](#)  
Formato de archivo: Desconocido - [Versión en HTML](#)  
# This is a basic ProFTPD configuration file (rename it to: # proftpd.conf for actual use. It establishes a single server. # and a single anonymous login ...  
[svn.wslm.org/share/Debian-Doc/manuals/debian-reference/.../proftpd.conf](#)

[trunk/configs/ubuntu/proftpd/proftpd.conf - ispCP Omega | ISP ...](#) [Traducir esta página](#)  
Revision 2505, 7.8 KB (checked in by nuwin, 8 days ago). Re-integration of the branch new-dbc in the current development branch : Command used: ...  
[isp-control.net/ispcp/browser/trunk/.../proftpd.conf](#) - [En caché](#) - [Similares](#) - [Traducir esta página](#)

Google intitle:"Mail Server CMailServer WebMail" "5.2"  [Advanced Search](#)

Web [Show options...](#) Results 1 - 3 of 3 for intitle:"Mail Server CMailServer WebMail" "5.2" (0.09 seconds)

[Mail Server CMailServer WebMail 5.2.1](#)  
New User! Sign Up Now! Username Password Save account and password. This mail server powered by Youngsoft.  
[web.uk.net/mail](#) - [Cached](#) - [Similar](#) - [Traducir esta página](#)

[Mail Server CMailServer WebMail 5.2.1](#)  
Sign up here. Username\*, Password\*, Confirm New Password\*, Your Name, Comment. Contact email. This mail server powered by Youngsoft.  
[web.uk.net/mail/signup.asp](#) - [Cached](#) - [Similar](#) - [Traducir esta página](#)

Sponsored Links  
[Complete Mail Server](#)  
Easy to install. Integrated webmail  
Fast. Stops spam and viruses  
[netwinste.com/surgemal.htm](#)  
[See your ad here >](#)

## Fase 1 (pre ataque)- *Footprinting*

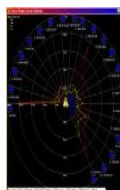
Obtener información inicial:

- whois
- nslookup

**InterNIC**

Localizar el rango de red:

- traceroute



# Whois

Registrant:  
targetcompany (targetcompany-ORG)  
100 Street  
# Street Address  
City, Province  
State, Pin, Country  
Domain Name: targetcompany.COM

**Registrant:**  
targetcompany (targetcompany-DOM)  
# Street Address  
City, Province  
State, Pin, Country  
**Domain Name: targetcompany.COM**

Administrative Contact:  
Surname, Name (SNIDNo-ORG) targetcompany@domain.com  
targetcompany (targetcompany-DOM) # Street Address  
City, Province, State, Pin, Country  
Telephone: XXXXXX Fax: XXXXXX

**Administrative Contact:**  
Surname, Name (SNIDNo-ORG) targetcompany@domain.com  
targetcompany (targetcompany-DOM) # Street Address  
City, Province, State, Pin, Country  
Telephone: XXXXXX Fax: XXXXXX

Technical Contact:  
Surname, Name (SNIDNo-ORG) targetcompany@domain.com  
targetcompany (targetcompany-DOM) # Street Address  
City, Province, State, Pin, Country  
Telephone: XXXXXX Fax: XXXXXX

**Technical Contact:**  
Surname, Name (SNIDNo-ORG) targetcompany@domain.com  
targetcompany (targetcompany-DOM) # Street Address  
City, Province, State, Pin, Country  
Telephone: XXXXXX Fax: XXXXXX

Domain servers in listed order:  
NS1.WEBHOST.COM XXX.XXX.XXX.XXX  
NS2.WEBHOST.COM XXX.XXX.XXX.XXX

Constanso Malaga NS2.WEBHOST.COM Módulo XXXXXXXXXX de formación  
Jesús Pancorbo

# Nslookup

```
jpancorb@calhost:~$
jpancorb@calhost:~$ nslookup
> set queryname
> oskius.com
Server:      80.58.61.250
Address:     80.58.61.250#53

Non-authoritative answer:
oskius.com  nameserver = dns1.peopleware.es.
oskius.com  nameserver = dns10.servidoresdns.net.
oskius.com  nameserver = dns2.peopleware.es.
oskius.com  nameserver = dns9.servidoresdns.net.

Authoritative answers can be found from:
dns10.servidoresdns.net internet address = 217.76.129.132
dns9.servidoresdns.net internet address = 217.76.128.132
> server dns1.peopleware.es
Default server: dns1.peopleware.es
Address: 82.229.182.117#53
> oskius.com
Server:      dns1.peopleware.es
Address:     82.229.182.117#53

oskius.com
origin = dns1.peopleware.es
mail addr = hostmaster.peopleware.es
serial = 2009070817
refresh = 21600
retry = 3600
expire = 2415000
minimum = 60400
oskius.com  nameserver = dns1.peopleware.es.
oskius.com  nameserver = dns2.peopleware.es.
Name:      oskius.com
Address:   217.76.130.14
oskius.com mail exchanger = 10 smtp-01.servidoresdns.net.
> www.oskius.com
Server:      dns1.peopleware.es
Address:     82.229.182.117#53

Name:      www.oskius.com
Address:   217.76.130.14
```

nslookup - resolución DNS  
(Sistema de Nombre de  
Dominios)

Con el nombre DNS de  
un equipo podemos  
obtener su ip.

Podemos obtener las ips  
de sus DNS internos.

Mediante sus DNS podemos  
obtener ips de sus máquinas  
web, de sus máquinas de mail,  
etc..

# Determinar el rango de red

## Incluiría:

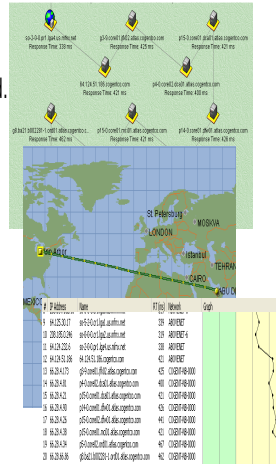
- Encontrar el rango de Ips.
- Encontrar la máscara de subred.
- Encontrar firewalls, DMZ, etc.

## Fuentes de información:

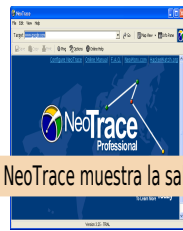
traceroute

## Hacking Tool:

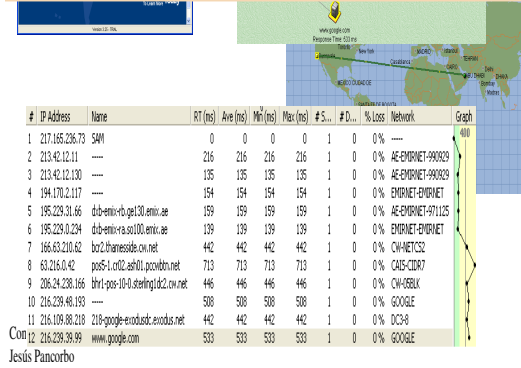
- NeoTrace / Geotrace.
- VisualRoute /Xroute (xt).
- Whatroute.



# Tool: NeoTrace (Now McAfee Visual Trace) - Geotrace (GNU)



NeoTrace muestra la salida de traceroute visualmente en un mapa.



Jesús Pancorbo



# Tool: VisualRoute Mail Tracker

Report for olympus.bic.nus.edu.sg [137.132.19.100]

Analysis: olympus.bic.nus.edu.sg was found in 24 hops (RTT=240). It is a SMTP server (ESMTP Sendmail 8.12.0/8.12.7).

MailTracker by Visiware

trwee@bic.nus.edu.sg

Server	Pin	P.Address	Status
olympus.bic.nus.edu.sg	10	137.132.19.100	ESMTP Sendmail 8.12.0/8.12.7

Click on a server name to start a VisualRoute trace

Hop	%Loss	IP Address	Node Name	Location	Tzone	rms	Graph	Network
0		217.165.221.153	SAM	*				Emirates Internet
1		213.42.12.6		(United Arab Emirates)		2537		Emirates Telecommunic
2		213.42.12.131		(United Arab Emirates)		2513		Emirates Telecommunic
3		194.170.2.117		(United Arab Emirates)		2467		Emirates Internet
4		195.229.31.35	auh-emi-rb.ge6303.er	(United Arab Emirates)		2429		Emirates Telecommunic
5		195.229.31.34	auh-emi-ra.ge6303.er	(United Arab Emirates)		2421		Emirates Telecommunic
6		62.216.144.25		(United Kingdom)		2766		FLAG Telecom Limited
7		62.216.140.9	ge-1-0-0.core1.sfr1.fr	(United Kingdom)		2894		FLAG Telecom Limited
8		166.90.133.105	giga4-1-116.ipoc02.Sa	San Francisco, CA, US	-08:00	2655		Level 3 Communications, In
9		200.244.14.201	giga4ethernet4-2.core	San Francisco, CA, US	-08:00	2695		Level 3 Communications, In
10		200.247.10.233	sa-4-0-0.mp2.SanFie	San Francisco, CA, US	-08:00	3008		Level 3 Communications, In

## Ejemplo

wikipedia.org

- whois - datos de la empresa. DNS de la empresa
- nslookup - sacar la IP de su servidor mail.
- traceroute - obtener la IP de su cortafuegos.