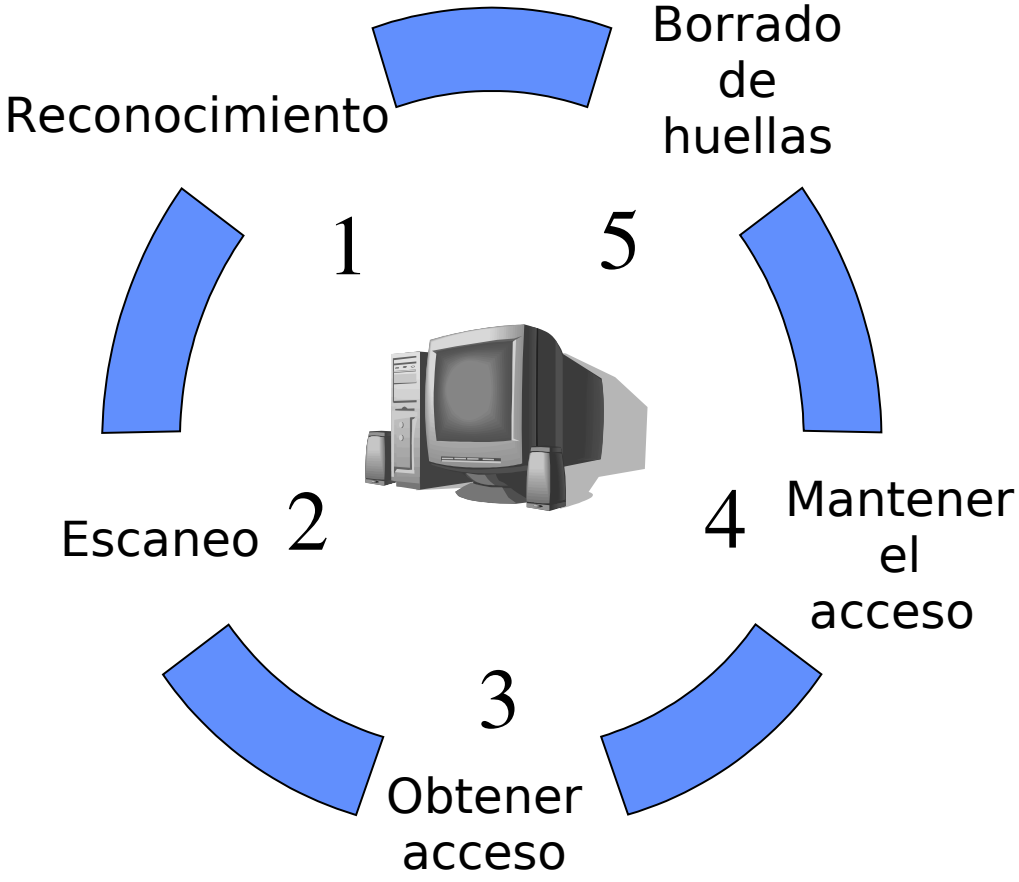
Hacking Ético

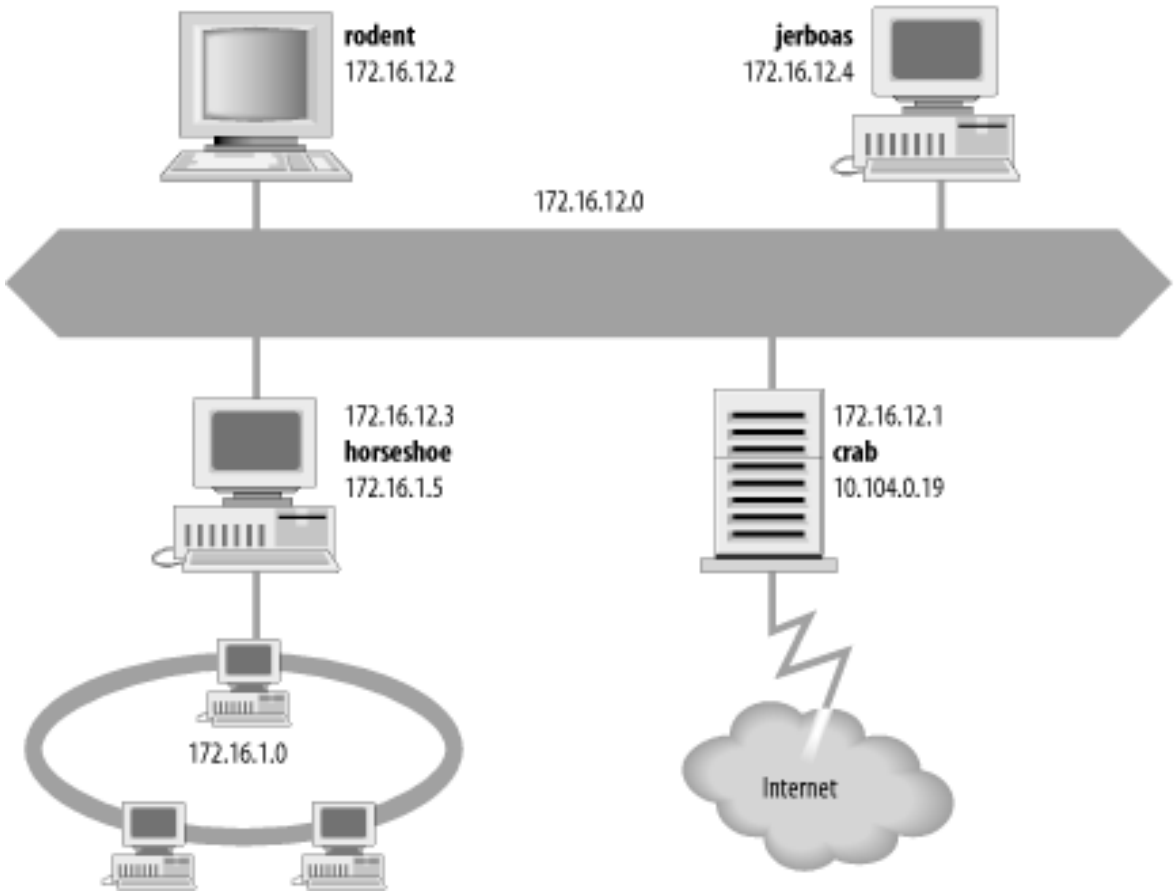
Módulo I

Fase 1: Obtención de información

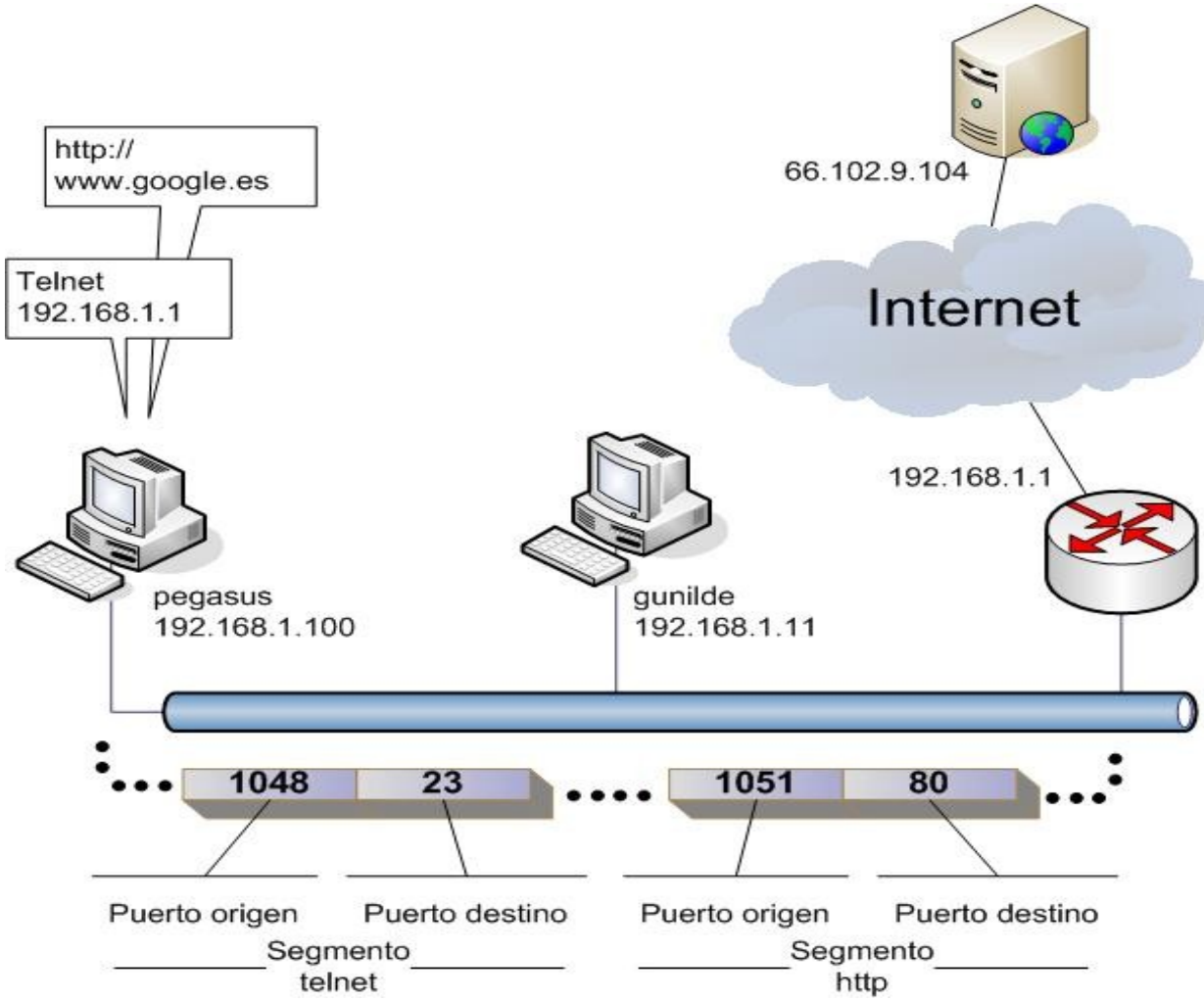
Obtención de información



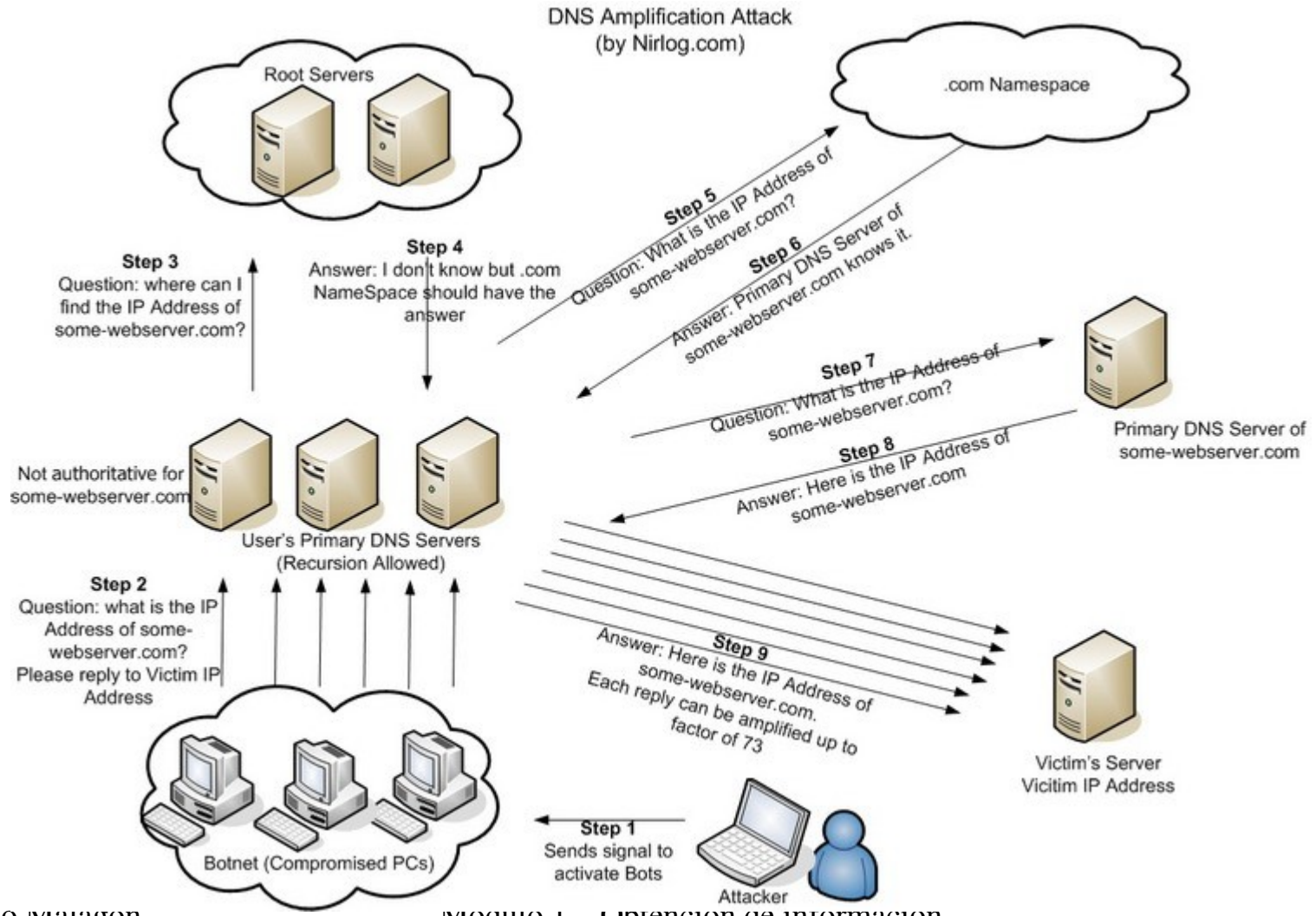
Conceptos: TCP/IP



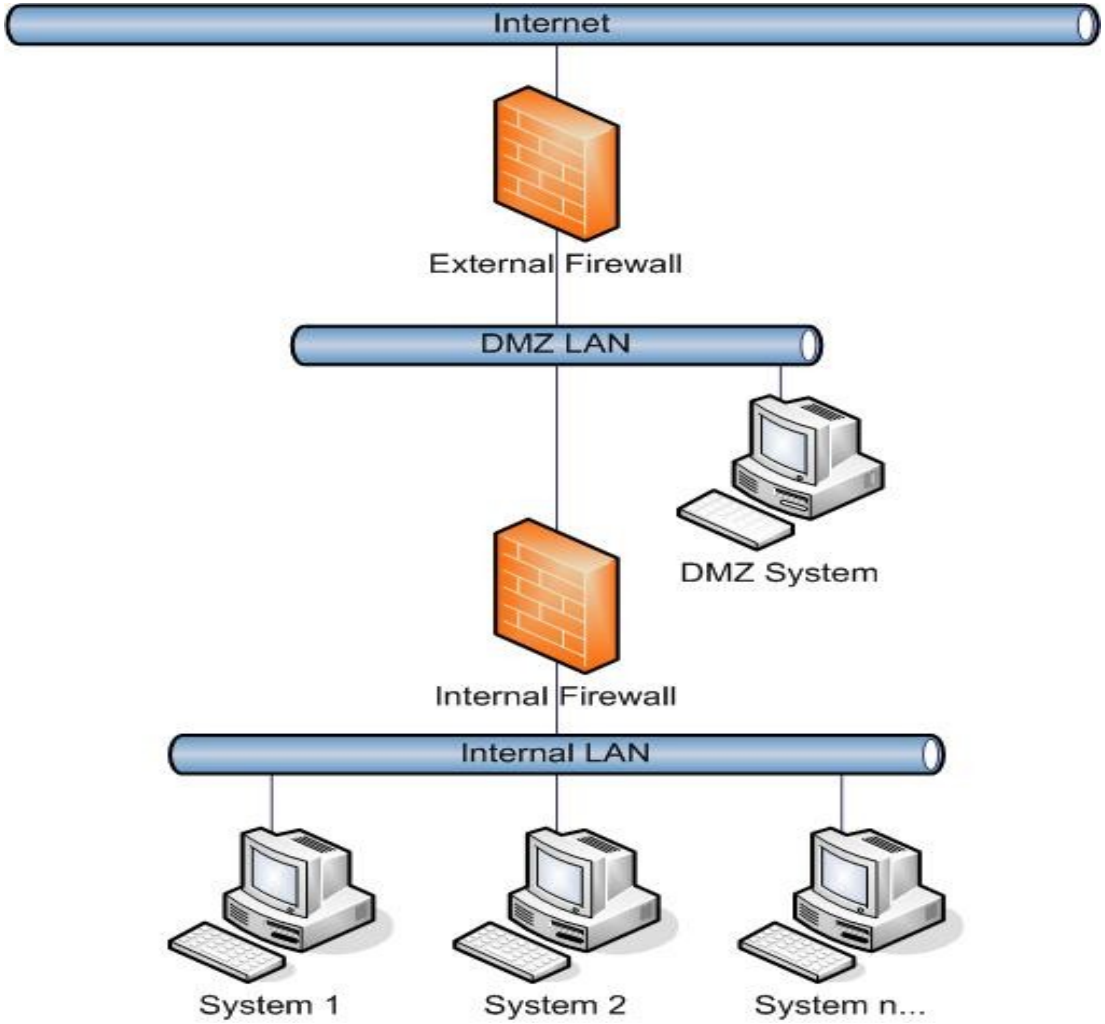
Conceptos: Servicio y Puerto



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:

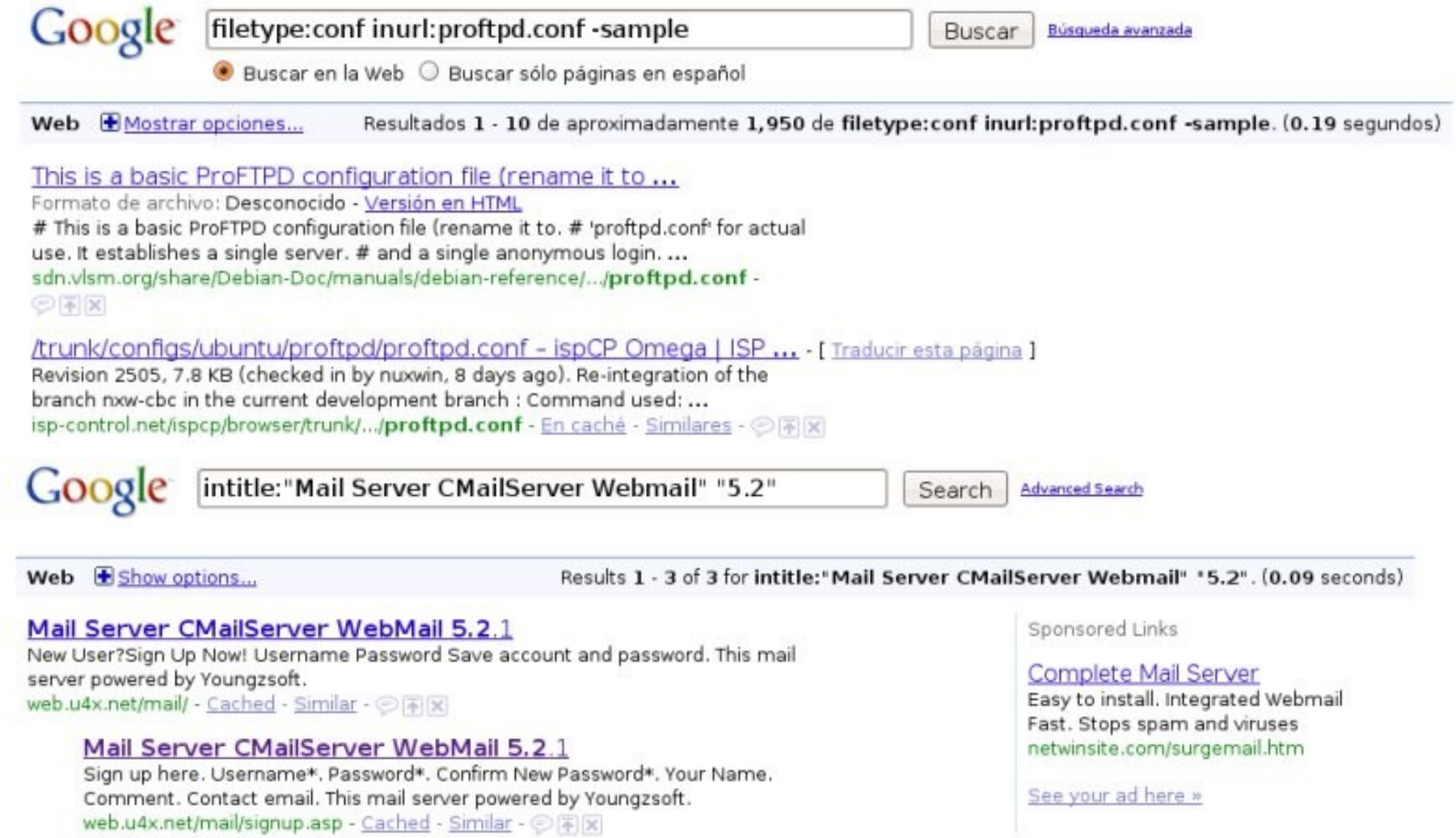
- Infojobs / monster
- Geogle hacking.
- Web de la empresa
- whois
- nslookup
- www.all-nettols.com

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



Fase 1 (pre ataque)- *Footprinting*

Obtener información inicial:

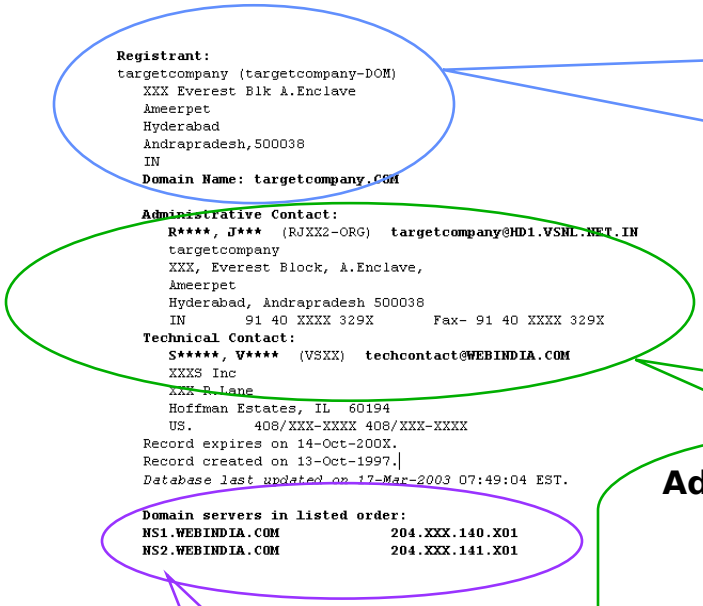
- whois
- nslookup

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

   Administrative Contact:
      R****, J***  (RJXX2-ORG)  targetcompany@HD1.VSNL.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
      XXXS 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.

   Domain servers in listed order:
   NS1.WEBINDIA.COM              204.XXX.140.X01
   NS2.WEBINDIA.COM              204.XXX.141.X01
```

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

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

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

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
> osmius.com
Server:         80.58.61.250
Address:        80.58.61.250#53

Non-authoritative answer:
osmius.com      nameserver = dns1.peopleware.es.
osmius.com      nameserver = dns10.servidoresdns.net.
osmius.com      nameserver = dns2.peopleware.es.
osmius.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
> osmius.com
Server:         dns1.peopleware.es
Address:        82.223.182.117#53

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

Name:   www.osmius.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:

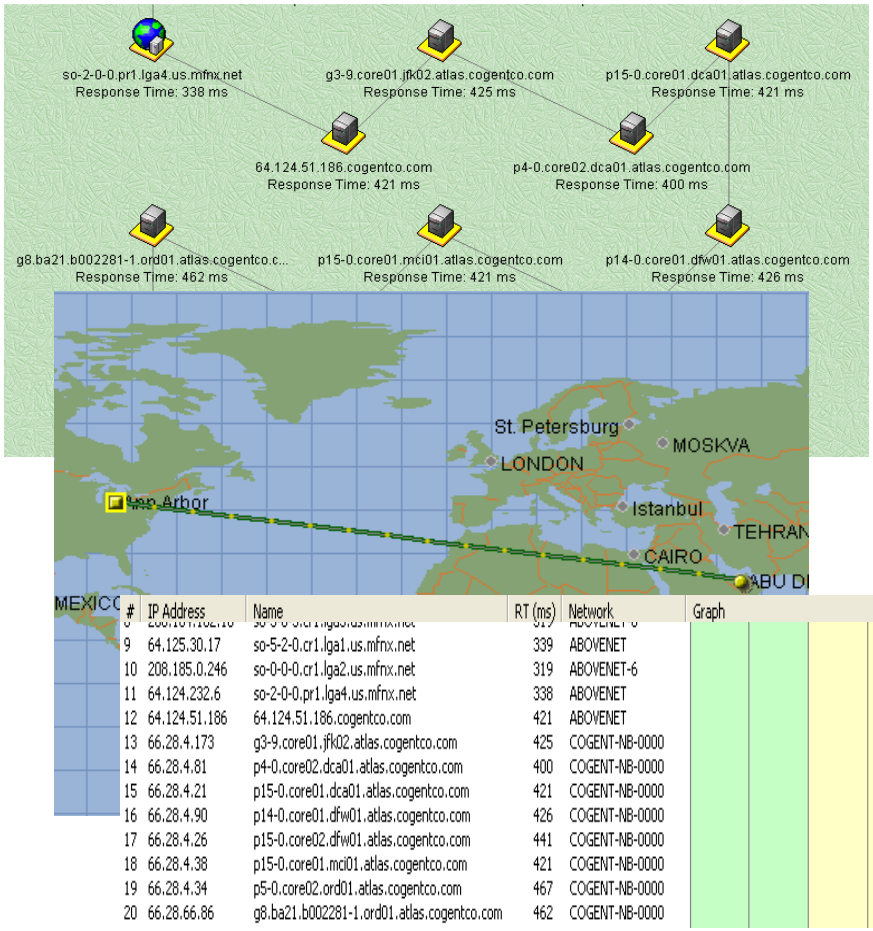
traceroute

Hacking Tool:

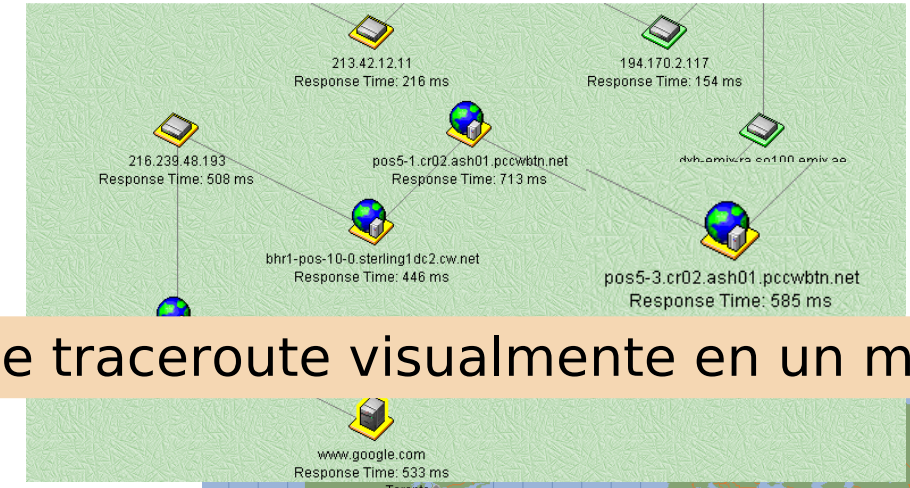
NeoTrace / Geotrace.

VisualRoute /Xroute (xt).

Whatroute.



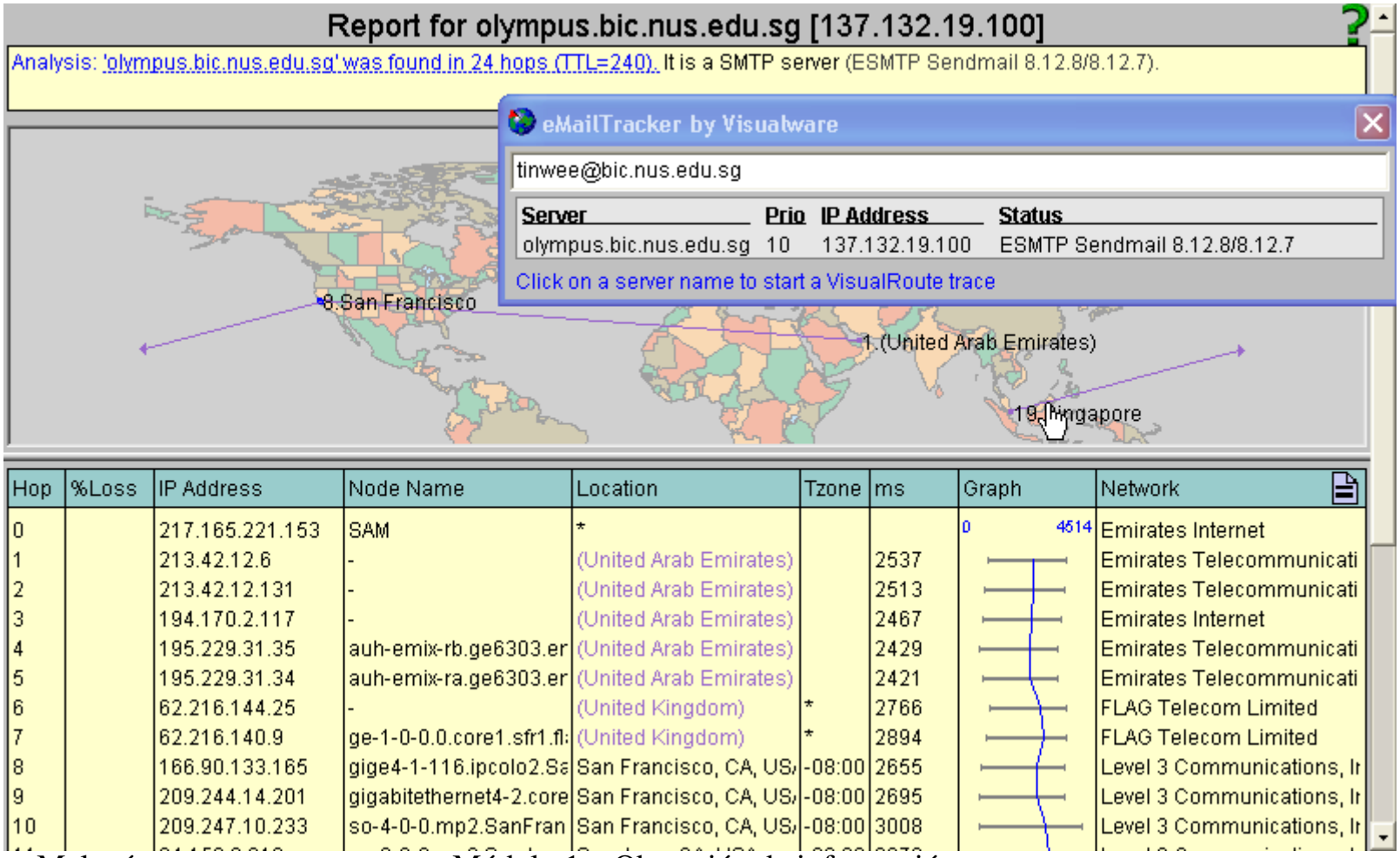
Tool: NeoTrace (Now McAfee Visual Trace) – Geotrace (GNU)



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 %	-----	400
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



Ejemplo

wikipedia.org

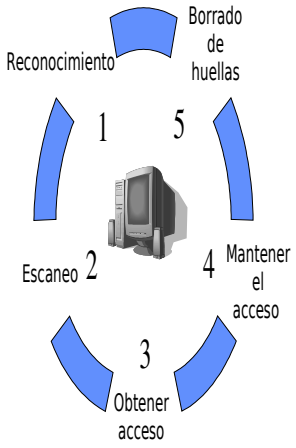
- whois – datos de la empresa. DNS de la empresa
- nslookup – sacar la IP de su servidor mail.
- traceroute – obtener la IP de su cortafuegos.

Hacking Ético

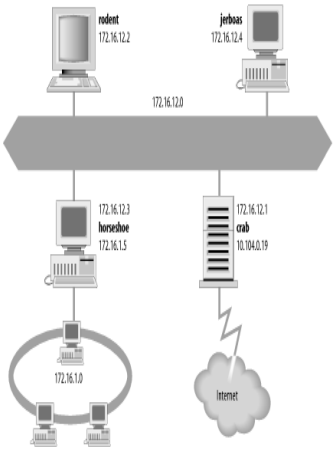
Módulo I

Fase 1: Obtención de información

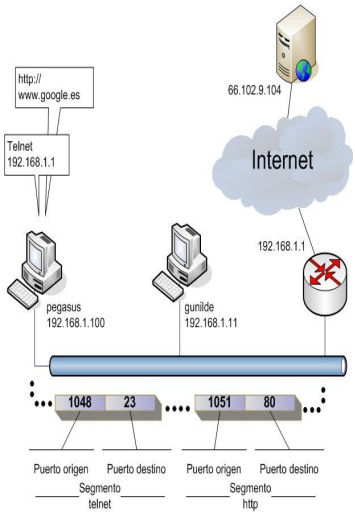
Obtención de información



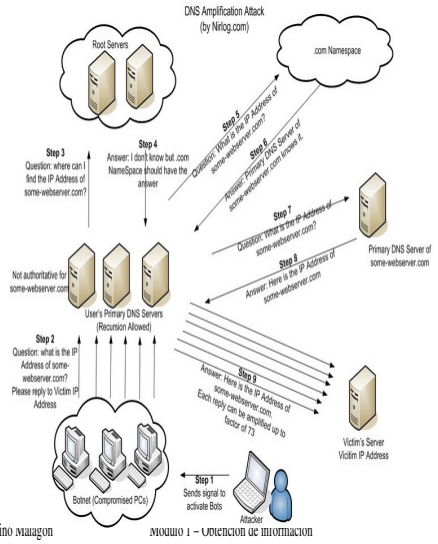
Conceptos: TCP/IP



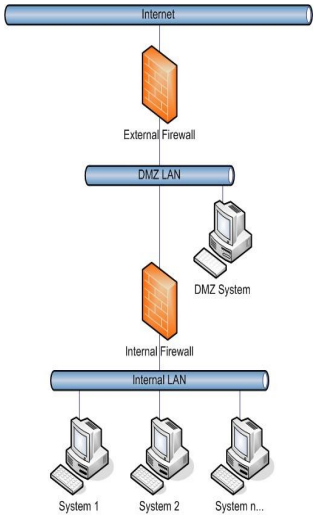
Conceptos: Servicio y Puerto



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
- Geogle hacking.
- Web de la empresa
- whois
- nslookup
- 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

Fase 1 (pre ataque)- *Footprinting*

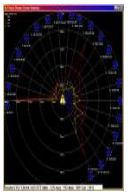
Obtener información inicial:

- whois
- nslookup

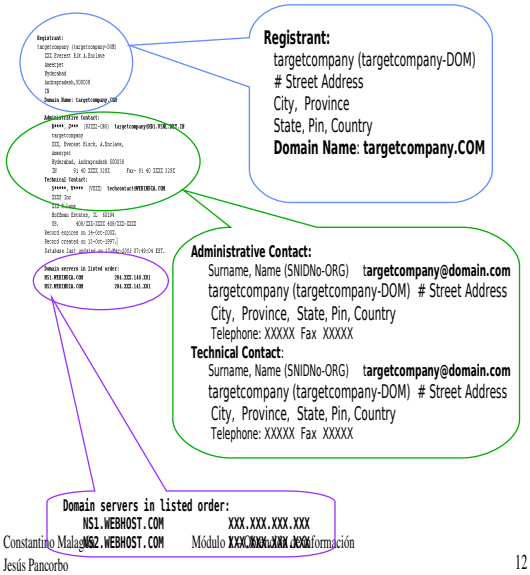
InterNIC

Localizar el rango de red:

- traceroute



Whois


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: 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.WEBHOST.COM XXX.XXX.XXX.XXX
NS2.WEBHOST.COM XXX.XXX.XXX.XXX

Nslookup

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

Non-authoritative answer:
osmius.com      nameserver = dns1.peopleware.es.
osmius.com      nameserver = dns10.servidoresdns.net.
osmius.com      nameserver = dns2.peopleware.es.
osmius.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
> osmius.com
Server:         dns1.peopleware.es
Address:        82.223.182.117#53

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

Name:   www.osmius.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:

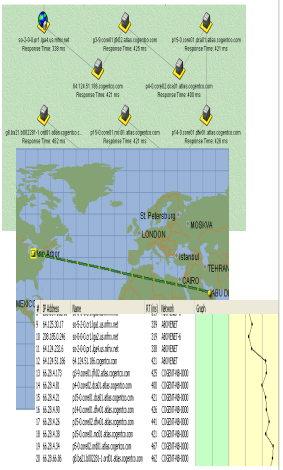
traceroute

Hacking Tool:

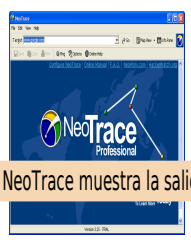
NeoTrace / Geotrace.

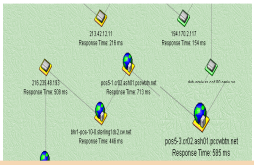
VisualRoute /Xroute (xt).

Whatroute.

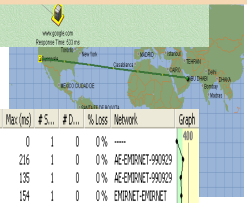


Tool: NeoTrace (Now McAfee Visual Trace) - Geotrace (GNU)



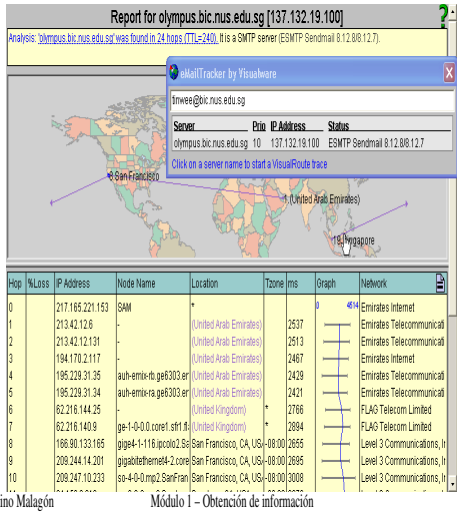


NeoTrace muestra la salida de traceroute visualmente en un mapa.



#	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 %	-----	400
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.pcvebtn.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



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.