



JUNTA DE ANDALUCÍA

CEP Lora del Río
CONSEJERÍA DE EDUCACIÓN

Curso de Seguridad y alta disponibilidad

CEP Lora del Río (Sevilla)

PENTEST 1



Licencia

Estas diapositivas han sido realizadas para el curso “Seguridad y Alta Disponibilidad” que se imparte a través del CEP de Lora del Río (Sevilla).

© José Ignacio Huertas, Alberto Molina Coballes
Septiembre 2013

Algunos derechos reservados. Este artículo se distribuye bajo la licencia “Reconocimiento-CompartirIgual 3.0 España” de Creative Commons, disponible en <http://creativecommons.org/licenses/by-sa/3.0/es/deed.es>





INTRODUCCIÓN

- **Importancia de los datos y servicios**
- **Es necesario evaluar la seguridad de nuestros sistemas.**
- **Objetivo de la primera parte del curso: Realizar un test de penetración (PenTest).**



INTRODUCCIÓN

○ Escenario “ficticio” de ataque de seguridad:

Un alumno/a de FP tiene como objetivo comprometer la seguridad de la red del centro.

- Recopila información de servidores DNS, máquinas activas, servidores Web, ..., con herramientas como nmap, dig, nslookup.
- Localiza información sobre el profesorado (Maltego, Foca,...): cuentas de correo, sistemas operativos, aplicaciones que usan,...
- Utiliza SET (Social Engineer Toolkit) para configurar un **clone-site attack** mediante un Applet firmado en Java.



INTRODUCCIÓN

- Manda un correo destinado a algún profesor/a animando a que haga clic en una URL que contiene información relacionada con algún tema en el que se encuentre trabajando.
- El remitente del correo sería falsificado por alguno que sea de confianza para la víctima, haciendo el correo más creíble.
- El profesor/a, tras leer el correo y hacer clic en la URL aceptaría el certificado firmado. Con esto el alumno obtendría una shell.



Contenido del día

- Ataques en redes de datos (PenTest)
 - **Búsqueda de información** ←
 - Búsqueda de vulnerabilidades
 - Explotar vulnerabilidades
- Configuraciones en Alta Disponibilidad



Contenido del día

- **Búsqueda de información:**
 - **Conceptos previos**
 - **¿Dónde está el enemigo?**
 - **Objetivos**
 - **Técnicas de Footprintig**
 - **Fingerprinting**



Conceptos previos

- **Auditoría de seguridad:** proceso que permite a una organización evaluar, de forma exhaustiva, el nivel de seguridad de sus sistemas informáticos. Identifica todos los posibles riesgos y su criticidad.
 - Caja negra: se realiza desde fuera
 - Caja blanca: desde dentro.
- **Test de intrusión (PenTest):** generalmente es un método de auditoría de caja negra que persigue llevar a cabo una intrusión.
- **Vulnerabilidad:** fallos de software que permiten a un atacante realizar una intrusión.



Conceptos previos

- Fases de un test de intrusión:
 - Contrato
 - Recogida de información
 - Footprinting
 - Fingerprinting
 - Análisis de vulnerabilidades
 - Explotación
 - Generación de informes para corregir los problemas



¿Dónde está el enemigo?

- Es necesario considerar cualquier escenario.
- Ataques internos vs ataques externos



Hacker



Ex empleado



Trabajador interno



OBJETIVOS

Objetivos de este primer día:

1. Escoger el punto de ejecución del test: usuario externo, cliente remoto, trabajador interno sin privilegios o bien con privilegios, ...
2. Buscar todos los activos de la empresa expuestos a nuestro punto de ejecución: servidores web, dns, fichero, correo, ...
3. Recoger TODA la información posible.



1. Búsqueda de información

- Búsqueda de información (**Information Gathering**): consiste en recolectar TODA la información posible del objetivo.
- **FootPrinting**: búsqueda “pasiva” de toda la información pública (por tanto es “legal”) sobre el sistema que se va a auditar, es decir, buscaremos todas las huellas posibles, desde direcciones IP, servidores internos, cuentas de correo, nombres de máquinas, información del registrador del dominio, tipos de servidores, ficheros con cuentas y/o credenciales de usuarios, impresoras, cámaras IP, metadatos, etc.



1. Búsqueda de información

- **FingerPrinting:** búsqueda “activa” de información. Para obtenerla se tiene que interactuar con los dispositivos. Para ello se le envía información y se analiza la respuesta recibida. Permite conocer: versiones de sistemas operativos, puertos abiertos, ...



1.1 Footprinting

- **Métodos:**
 - DNS
 - Tracear y posicionar
 - Whois
 - Netcraft
 - Búsqueda en buscadores
 - Metadatos
 - Spidering



1.1.1 DNS

- Nos podrá dar información del direccionamiento IP, servidores, servicios, ...
- Técnicas:
 - Forzar transferencias de zona
 - Realizar consultas inversas PTR para descubrir máquinas y servicios.
 - Ataque de fuerza bruta o diccionario.



1.1.1 DNS: transferencia de zona

○ Desde windows mediante nslookup:

- Inicio – Ejecutar – cmd
- nslookup
- set type=ns
- <dominio_victima>
- server <servidor_dns_victima>
- set type=all
- ls <dominio_victima>



1.1.1 DNS – Forzar transferencia de zona

```
F:\>nslookup
Servidor predeterminado: [redacted]
Address: [redacted]
```

```
> set type=ns
> uam.es
Servidor: [redacted]
Address: [redacted]
```

```
Respuesta no autoritativa:
uam.es nameserver = ns.uam.es
uam.es nameserver = ns0.uam.es
uam.es nameserver = ns2.uam.es
```

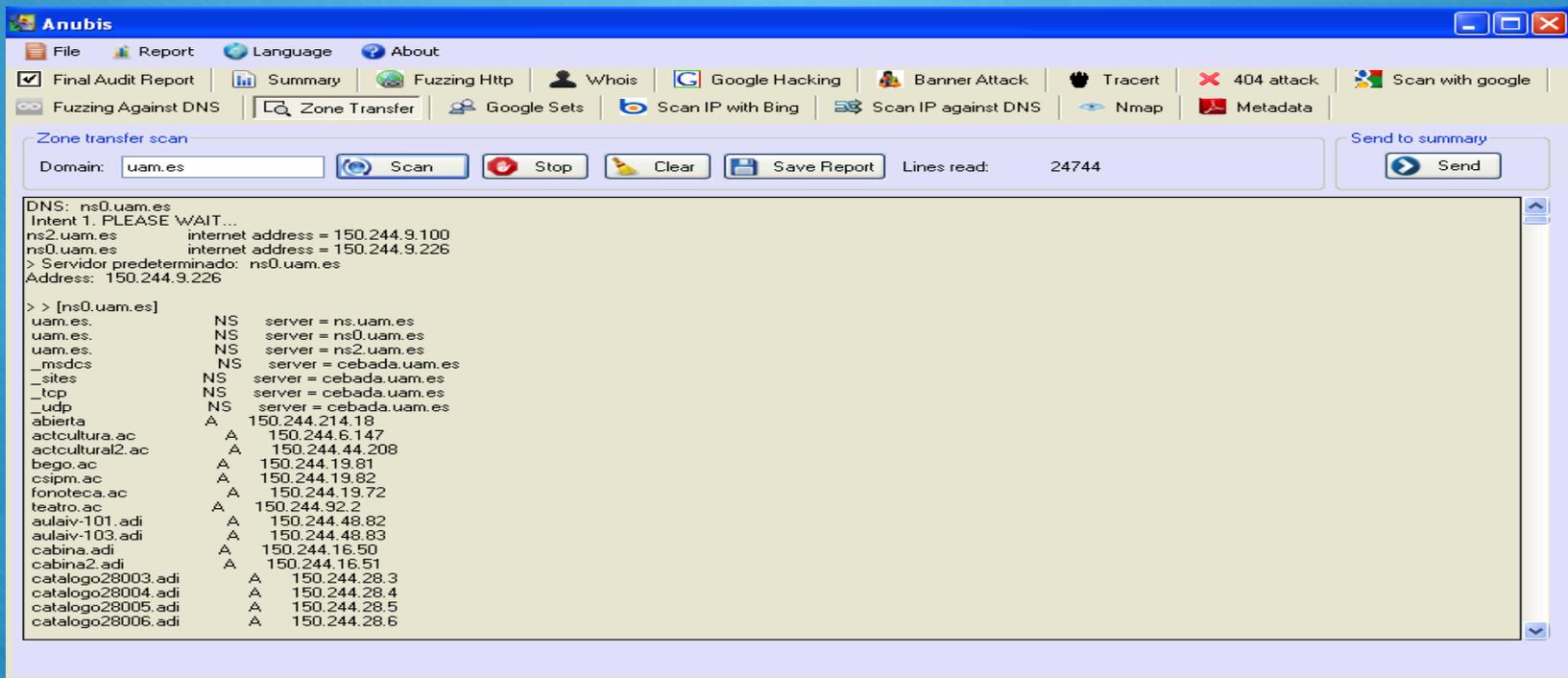
```
ns0.uam.es internet address
ns2.uam.es internet address
> server ns0.uam.es
Servidor predeterminado: ns0.uam
Address: 150.244.9.226
```

```
> set type=all
>
>
```

```
C:\WINDOWS\system32\cmd.exe - nslookup
> ls uam.es
[ns0.uam.es]
uam.es NS server = ns.uam.es
uam.es NS server = ns0.uam.es
uam.es NS server = ns2.uam.es
_msdc NS server = cebada.uam.es
_sites NS server = cebada.uam.es
_tcp NS server = cebada.uam.es
_udp NS server = cebada.uam.es
abierta A 150.244.214.18
actcultura.ac A 150.244.6.147
actcultural2.ac A 150.244.44.208
bego.ac A 150.244.19.81
csipm.ac A 150.244.19.82
fonoteca.ac A 150.244.19.72
teatro.ac A 150.244.92.2
aulaiv-101.adi A 150.244.48.82
aulaiv-103.adi A 150.244.48.83
cabina.adi A 150.244.16.50
cabina2.adi A 150.244.16.51
catalogo28003.adi A 150.244.28.3
catalogo28004.adi A 150.244.28.4
catalogo28005.adi A 150.244.28.5
catalogo28006.adi A 150.244.28.6
catalogo28007.adi
```



1.1.1 DNS – Forzar transferencia de zona



The screenshot shows the Anubis web application interface. The main window displays the results of a Zone Transfer scan for the domain uam.es. The interface includes a menu bar with options like File, Report, Language, and About. Below the menu, there are several tool buttons such as Final Audit Report, Summary, Fuzzing Http, Whois, Google Hacking, Banner Attack, Tracert, 404 attack, Scan with google, Fuzzing Against DNS, Zone Transfer, Google Sets, Scan IP with Bing, Scan IP against DNS, Nmap, and Metadata. The Zone Transfer scan section shows the domain uam.es and the scan results.

```
DNS: ns0.uam.es
Intent 1. PLEASE WAIT...
ns2.uam.es      internet address = 150.244.9.100
ns0.uam.es     internet address = 150.244.9.226
> Servidor predeterminado: ns0.uam.es
Address: 150.244.9.226

> > [ns0.uam.es]
uam.es.        NS      server = ns.uam.es
uam.es.        NS      server = ns0.uam.es
uam.es.        NS      server = ns2.uam.es
_uamdcns      NS      server = cebada.uam.es
_sites        NS      server = cebada.uam.es
_tcp          NS      server = cebada.uam.es
_udp          NS      server = cebada.uam.es
abierta       A       150.244.214.18
actcultura.ac A       150.244.6.147
actcultural2.ac A      150.244.44.208
bego.ac       A       150.244.19.81
csipm.ac      A       150.244.19.82
fonoteca.ac   A       150.244.19.72
teatro.ac     A       150.244.92.2
aulaiv-101.adi A      150.244.48.82
aulaiv-103.adi A      150.244.48.83
cabina.adi    A       150.244.16.50
cabina2.adi   A       150.244.16.51
catalogo28003.adi A      150.244.28.3
catalogo28004.adi A      150.244.28.4
catalogo28005.adi A      150.244.28.5
catalogo28006.adi A      150.244.28.6
```



1.1.1 DNS – Resolución inversa (PTR Scan)

○ Desde windows mediante nslookup:

- Inicio – Ejecutar – cmd
- nslookup
- set type=ns
- <dominio_victima>
- server <servidor_dns_victima>
- set type=ptr
- <ip_a_probar>

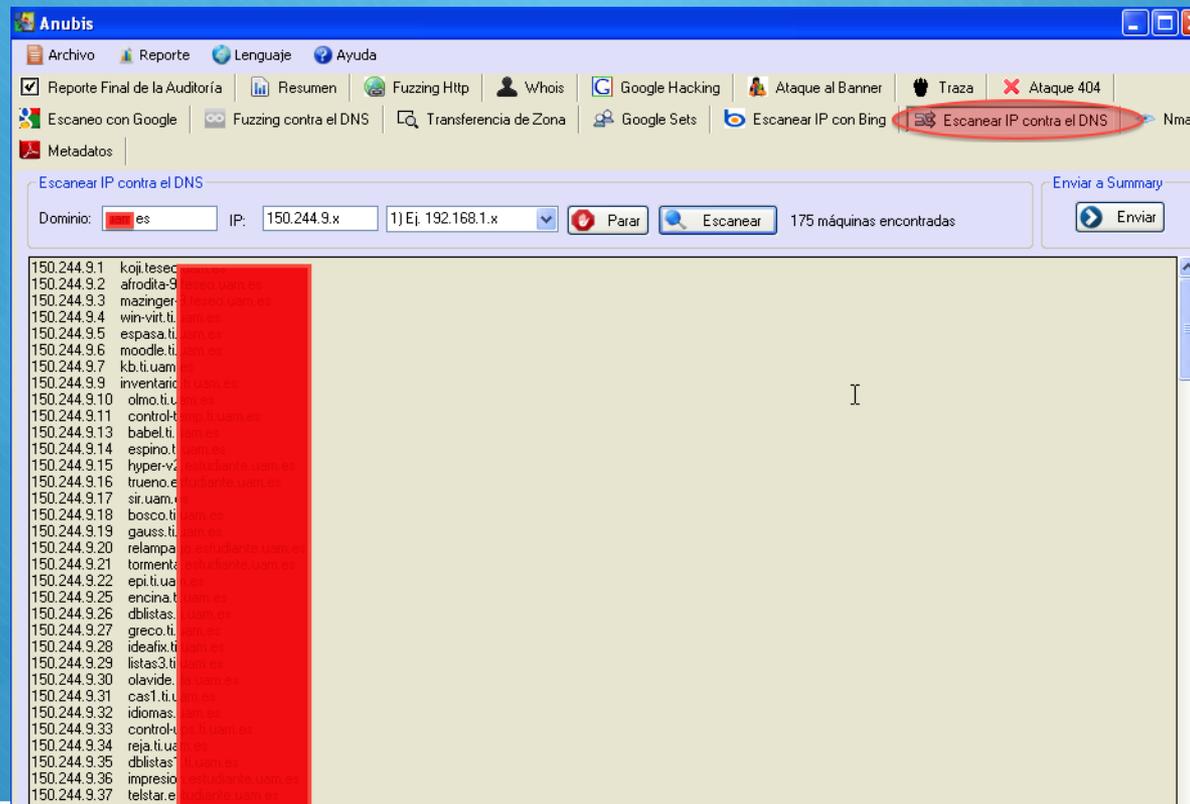


1.1.1 DNS – Resolución inversa

- Habría que repetir este proceso con todas las ip de un rango.
- Aplicación que automatice esta tarea: Foca, Anubis.



1.1.1 DNS – Resolución inversa



The screenshot shows the Anubis web application interface. The main menu includes options like 'Reporte Final de la Auditoría', 'Resumen', 'Fuzzing Http', 'Whois', 'Google Hacking', 'Ataque al Banner', 'Traza', and 'Ataque 404'. A red circle highlights the 'Escanear IP contra el DNS' option in the menu. Below the menu, the 'Escanear IP contra el DNS' section is active, showing a search for the domain 'es' with IP ranges '150.244.9.x' and '1|Ej: 192.168.1.x'. The results show a list of IP addresses and their corresponding hostnames, such as '150.244.9.1 koji.tesec.es' and '150.244.9.2 afrodita-9.es'. A red vertical bar highlights the first column of the results.

IP	Host
150.244.9.1	koji.tesec.es
150.244.9.2	afrodita-9.es
150.244.9.3	mazingera.es
150.244.9.4	win-virt.ti.es
150.244.9.5	espasa.ti.es
150.244.9.6	moodle.ti.es
150.244.9.7	kb.ti.uam.es
150.244.9.9	inventario.ti.es
150.244.9.10	olmo.ti.uam.es
150.244.9.11	control-ti.es
150.244.9.13	babel.ti.es
150.244.9.14	espino.ti.es
150.244.9.15	hyper-v.ti.es
150.244.9.16	trueno.es
150.244.9.17	sir.uam.es
150.244.9.18	bosco.ti.es
150.244.9.19	gauss.ti.es
150.244.9.20	relampago.es
150.244.9.21	tormento.es
150.244.9.22	epi.ti.uam.es
150.244.9.25	encina.ti.es
150.244.9.26	dblistas.es
150.244.9.27	greco.ti.es
150.244.9.28	ideafix.ti.es
150.244.9.29	listas3.ti.es
150.244.9.30	olavide.ti.es
150.244.9.31	cas1.ti.uam.es
150.244.9.32	idiomas.ti.es
150.244.9.33	control-ti.es
150.244.9.34	reja.ti.uam.es
150.244.9.35	dblistas.es
150.244.9.36	impresio.es
150.244.9.37	telstar.es

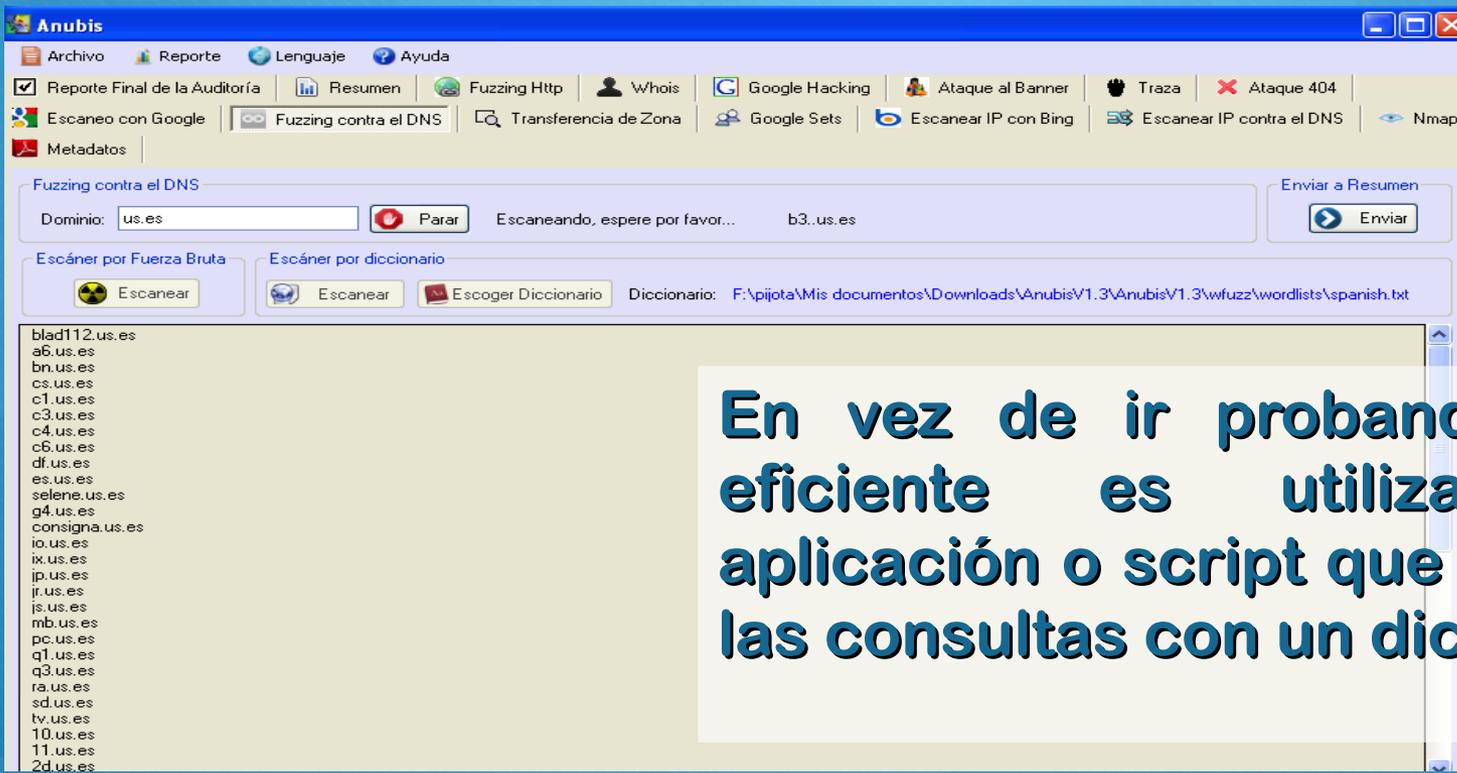


1.1.1 DNS – Fuerza bruta / diccionario

- Desde windows mediante nslookup:
 - Inicio – Ejecutar – cmd
 - nslookup
 - set type=ns
 - <dominio_victima>
 - server <servidor_dns_victima>
 - set type=a
 - <nombre_a_probar>



1.1.1 DNS – Fuerza bruta / diccionario



The screenshot shows the Anubis web application interface. At the top, there are navigation links: Archivo, Reporte, Lenguaje, and Ayuda. Below these are various tool buttons: Reporte Final de la Auditoría, Resumen, Fuzzing Htp, Whois, Google Hacking, Ataque al Banner, Traza, Ataque 404, Escaneo con Google, Fuzzing contra el DNS, Transferencia de Zona, Google Sets, Escanear IP con Bing, Escanear IP contra el DNS, and Nmap. The main section is titled 'Fuzzing contra el DNS' and contains a form with 'Dominio: us.es' and a 'Parar' button. Below this, there are two tabs: 'Escanear por Fuerza Bruta' and 'Escanear por diccionario'. The 'Escanear por diccionario' tab is active, showing a list of scanned domains and a dictionary path: 'Diccionario: F:\pipjota\Mis documentos\Downloads\AnubisV1.3\AnubisV1.3\wfuzz\wordlists\spanish.txt'. The list of domains includes: blad112.us.es, a6.us.es, bn.us.es, cs.us.es, c1.us.es, c3.us.es, c4.us.es, c6.us.es, df.us.es, es.us.es, selene.us.es, g4.us.es, consigna.us.es, io.us.es, ix.us.es, jp.us.es, jr.us.es, js.us.es, mb.us.es, pc.us.es, q1.us.es, q3.us.es, ra.us.es, sd.us.es, tv.us.es, 10.us.es, 11.us.es, and 2d.us.es.

En vez de ir probando, lo más eficiente es utilizar alguna aplicación o script que automatice las consultas con un diccionario.



1.1.1 DNS Cache Snooping

- Consiste en forzar la consulta de la caché de un servidor DNS. Con ello sabremos si algún cliente ha consultado previamente alguna web.
- Desde windows mediante nslookup:
 - Inicio – Ejecutar – cmd
 - nslookup
 - set type=ns
 - <dominio_victima>
 - server <servidor_dns_victima>
 - set type=a
 - set norecurse
 - <nombre_a_probar>

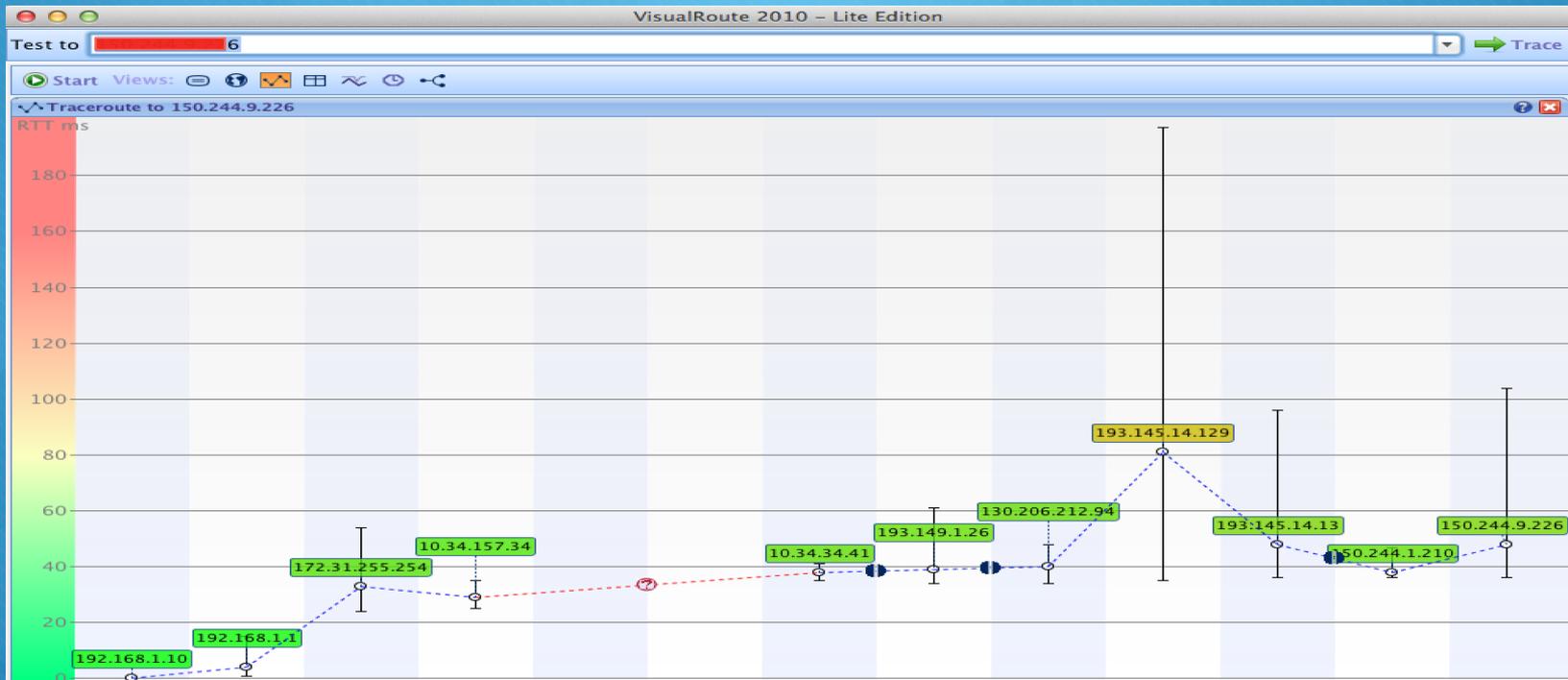


1.1.2 Tracear y posicionar

- Una vez obtenidos los objetivos con sus correspondientes Ips habría que situarlos en la red y posicionarlos geográficamente.
- Aplicaciones: tracert, **visualroute**, ...



1.1.2 Tracear y posicionar





1.1.3 Whois

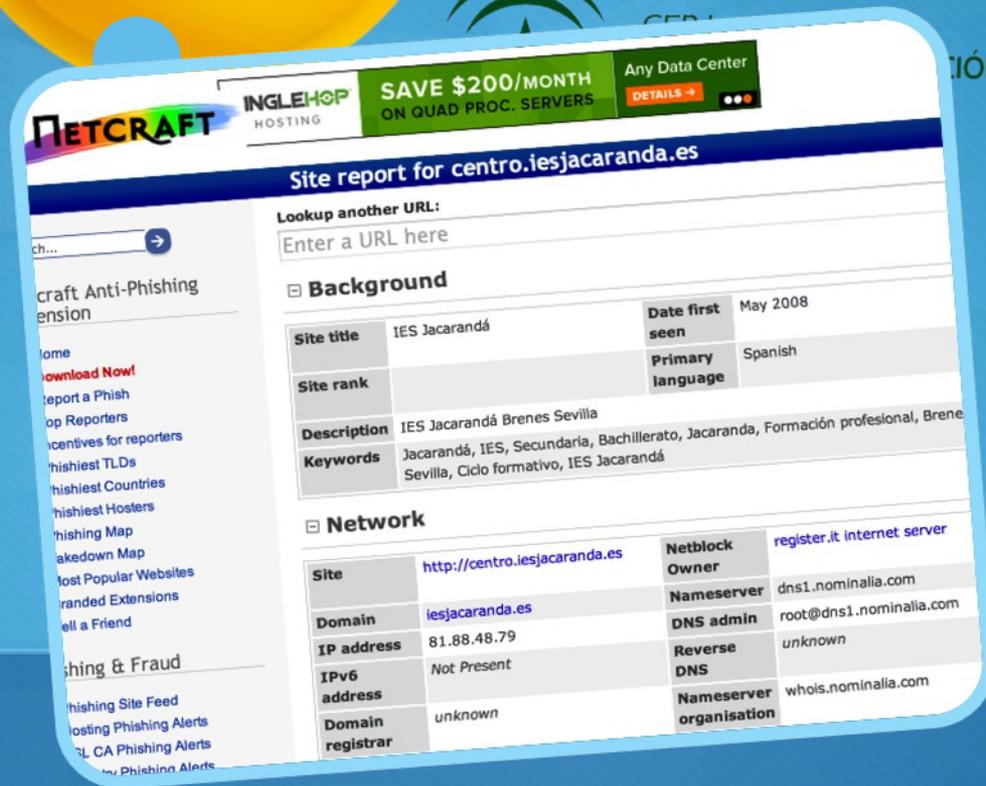
- Cuando una empresa adquiere un dominio en Internet, una serie de datos en Internet deben estar en una base de datos pública y esta información que se puede consultarla.
- Por defecto esta información está en una base de datos pública y esta información que se puede consultarla.



Buscador de Dominios (WHOIS) -
www.chatox.com/whois/whois.php

La Empresa
Buscado: 'loracep.org' - El dominio está a

```
Domain Name:LORACEP.ORG
Created On:20-Mar-2003 18:12:30 UTC
Last Updated On:19-Feb-2013 05:35:21 UT
Expiration Date:20-Mar-2015 18:12:30 UT
Sponsoring Registrar:Network Solutions
Status:OK
Registrant ID:34818786-NSI
Registrant Name:CENTRODEPROFESORADO DE
Registrant Organization:CENTRODEPROFESOR
O
Registrant Street1:C Blas Infante 14
Registrant Street2:
Registrant Street3:
Registrant City:LORA DEL RIO
Registrant State/Province:
Registrant Postal Code:41440
Registrant Country:ES
Registrant Phone:+1.34955801989
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:cepse6.cec@juntadeand
Admin ID:34818786-NSI
Admin Name:CENTRODEPROFESORADO DE LORA
Admin Organization:CENTRODEPROFESORADO
Admin Street1:C Blas Infante 14
Admin Street2:
Admin Street3:
Admin City:LORA DEL RIO
Admin State/Province:
Admin Postal Code:41440
Admin Country:ES
Admin Phone:+1.34955801989
Admin Phone Ext.:
Admin FAX:
Admin FAX Ext.:
Admin Email:cepse6.cec@juntadeandalucia
Tech ID:21244476-NSI
```



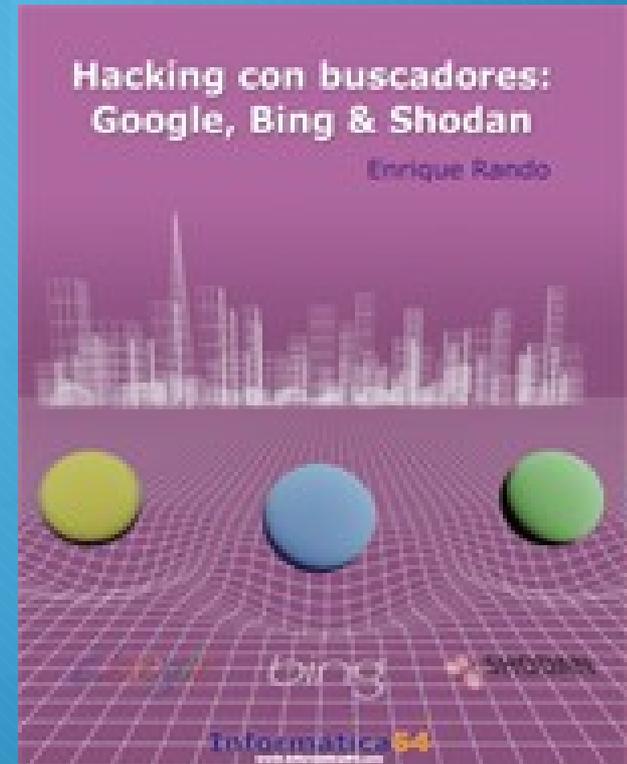
1.1.4 Netcraft

Hay sitios webs que nos permiten obtener información acerca de un dominio.



1.1.5 A través de buscadores

- Existe mucha información que han indexado los buscadores y que está disponible públicamente para su consulta. Tan sólo hay que saber qué preguntar a los buscadores.
- Etiquetas: site, inurl, intitle, ...
- Anubis – Google Hacking
- <http://www.exploit-db.com/google-dorks/>





1.1.6 Metadatos

- Datos que son almacenados junto con los documentos para ayudar en su identificación.
- Contienen mucha información: usuario que ha creado el archivo, impresoras, ubicaciones de red, ...
- Ejemplos de importancia: Blair, hacker y su novia



1.1.7 Spidering

- Las técnicas de Spidering se utilizan para poder encontrar toda la información que se ofrece gratuitamente a través de los sitios web de la compañía. Se recopilan páginas html, ficheros de imágenes, documentos, javascripts, applets, etc...



<http://www.informatica64.com/foca.aspx>



1.2 FingerPrinting

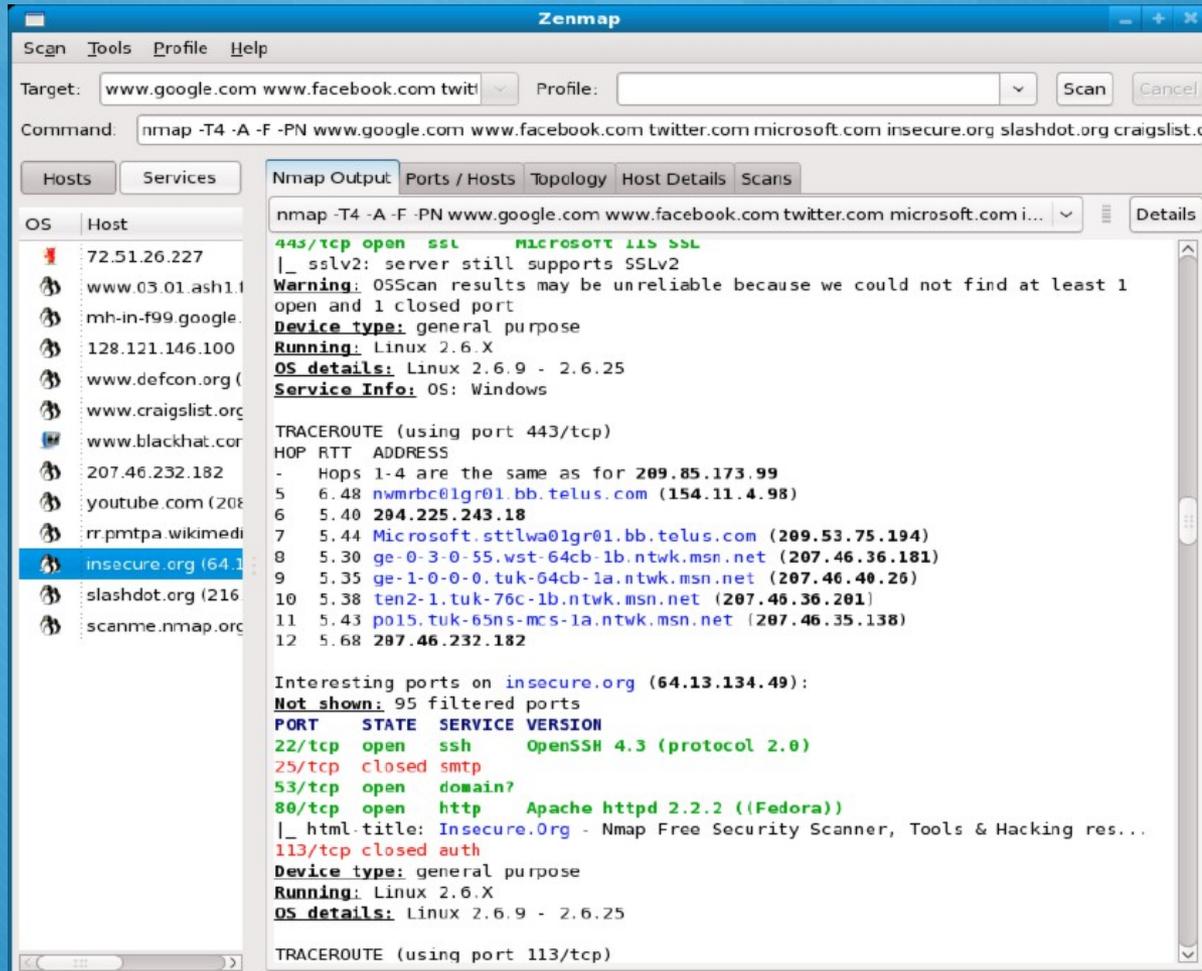
- Una vez que hemos recogido toda la información que era pública, ahora vamos a recoger aquella que también está accesible públicamente pero que a priori no se puede ver.
- Vamos a ir realizando pruebas a cada uno de los servicios y o servidores para obtener más información.





1.2 FingerPrinting

- Aplicaciones de escaneo: ¿Sistemas operativos, dispositivos de red, firewalls, puertos abiertos, ...?
- El objetivo de los métodos de escaneo es averiguar todos los puertos que se encuentran ofreciendo servicio por TCP/UDP sin levantar alarmas y dejar el menor rastro posible.
- Nmap, Zenmap

Zenmap

Scan Tools Profile Help

Target: Profile: Scan Cancel

Command: `nmap -T4 -A -F -PN www.google.com www.facebook.com twitter.com microsoft.com insecure.org slashdot.org craigslist.c`

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS	Host
	72.51.26.227
	www.03.01.ash1
	mh-in-f99.google
	128.121.146.100
	www.defcon.org (
	www.craigslist.org
	www.blackhat.cor
	207.46.232.182
	youtube.com (208
	rr.pmtpa.wikimedi
	insecure.org (64.1
	slashdot.org (216
	scanme.nmap.org

Nmap Output Ports / Hosts Topology Host Details Scans

`nmap -T4 -A -F -PN www.google.com www.facebook.com twitter.com microsoft.com i...` Details

```

443/tcp open  ssl      MICROSOFT IIS SSL
|_ sslv2: server still supports SSLv2
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.25
Service Info: OS: Windows

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
- Hops 1-4 are the same as for 209.85.173.99
5 6.48 nwmrbc@lgr01.bb.telus.com (154.11.4.98)
6 5.40 204.225.243.18
7 5.44 Microsoft.sttlwa0lgr01.bb.telus.com (209.53.75.194)
8 5.30 ge-0-3-0-55.wst-64cb-1b.ntwk.msn.net (207.46.36.181)
9 5.35 ge-1-0-0-0.tuk-64cb-1a.ntwk.msn.net (207.46.40.26)
10 5.38 ten2-1.tuk-76c-1b.ntwk.msn.net (207.46.36.201)
11 5.43 po15.tuk-65ns-mcs-1a.ntwk.msn.net (207.46.35.138)
12 5.68 207.46.232.182

Interesting ports on insecure.org (64.13.134.49):
Not shown: 95 filtered ports
PORT STATE SERVICE VERSION
22/tcp open  ssh      OpenSSH 4.3 (protocol 2.0)
25/tcp closed smtp
53/tcp open  domain?
80/tcp open  http     Apache httpd 2.2.2 ((Fedora))
|_ html-title: Insecure.Org - Nmap Free Security Scanner, Tools & Hacking res...
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.25

TRACEROUTE (using port 113/tcp)

```



TAREA 1: Obteniendo información

- Utilizando los métodos vistos hasta ahora, realiza la búsqueda de información más detallada posible de algún dominio y haz una interpretación de los datos obtenidos.



Fuentes:

- http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_information_gathering.pdf
- <http://www.flu-project.com/la-biblia-del-footprinting-i-de-vii.html>
- <http://www.elladodelmal.com/2007/02/test-de-intrusion-i-de-vi.html>
- <http://www.slideshare.net/jmorenol/test-de-intrusion-i-intelligence-gathering>
- <http://0xword.com/>