CEP Lora del Río
CONSEJERÍA DE EDUCACIÓN

Curso de Seguridad y alta disponibilidad

CEP Lora del Río (Sevilla)

PENTEST 1

JUNTA DE ANDALUCIA
CEP Lora del Río
CONSEJERÍA DE EDUCACIÓN

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).

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>

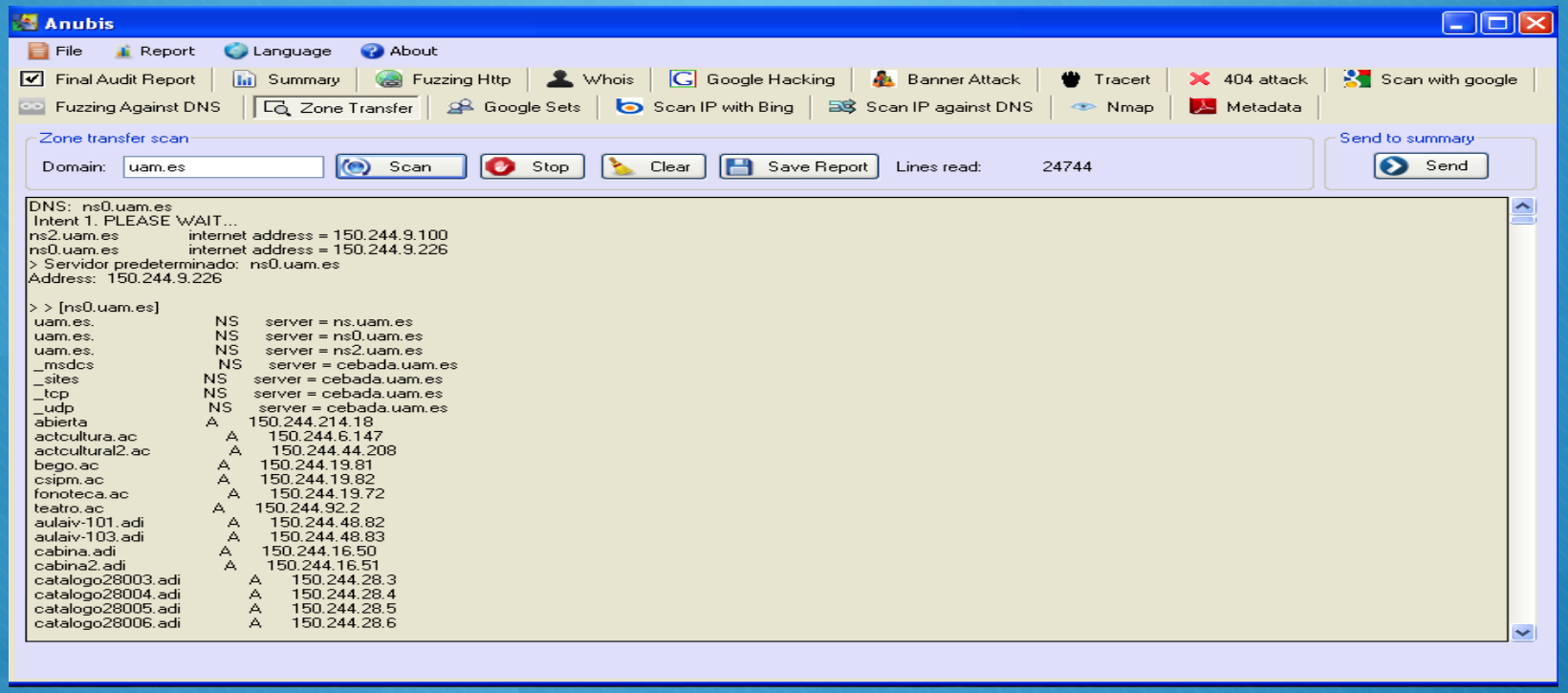
1.1.1 DNS – Forzar transferencia de zona

```
F:\[redacted]>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 [redacted]
ns2.uam.es      internet address [redacted]
> 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
 _msdcs                         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
 actcultura12.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



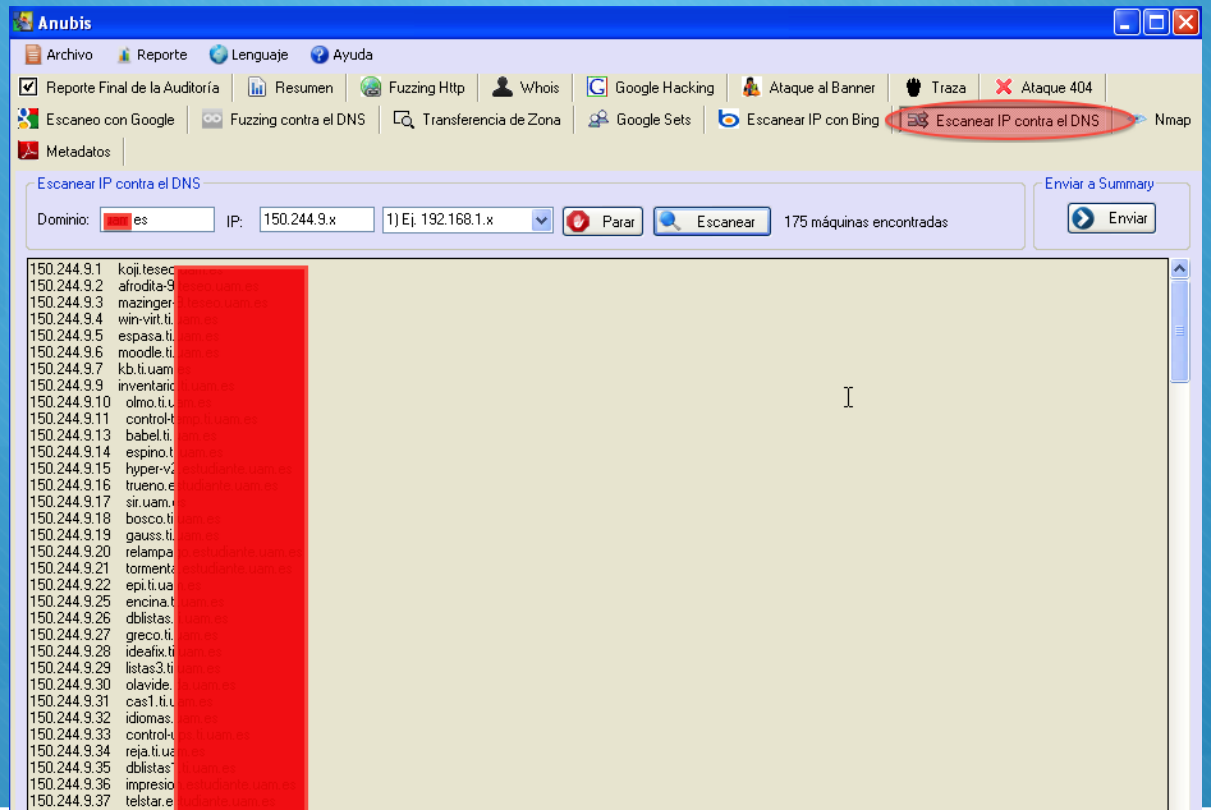
1.1.1 DNS – Resolución inversa (PTR Scan)

- 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.

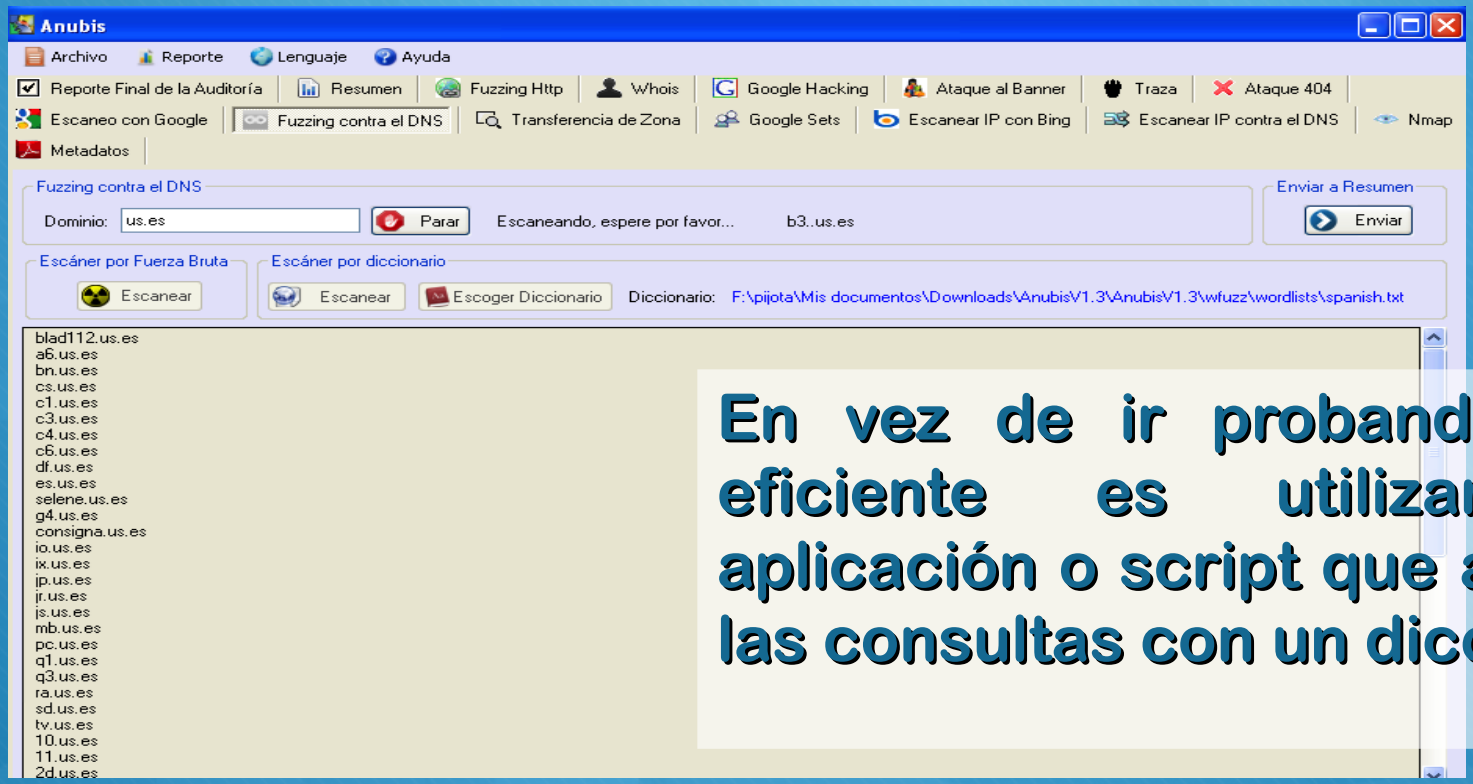
1.1.1 DNS – Resolución inversa



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



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

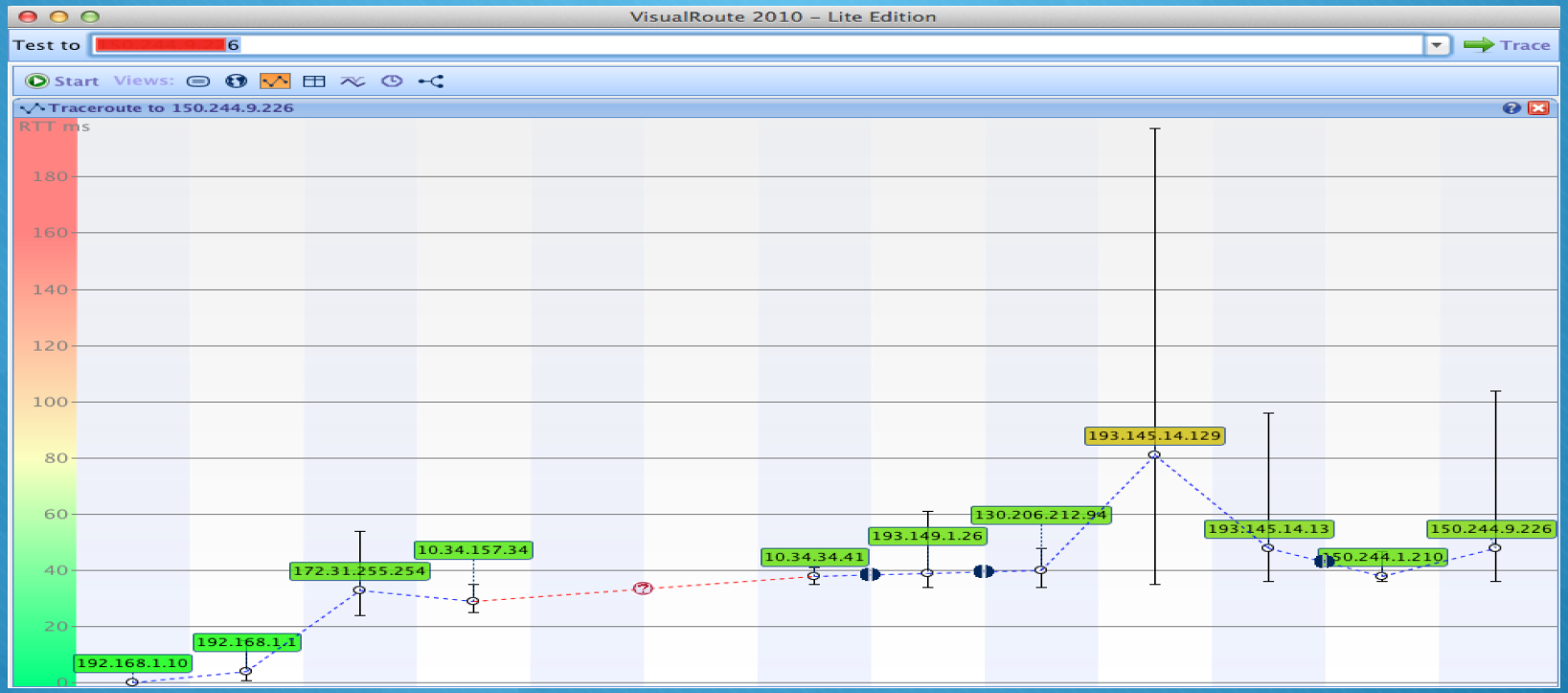
1.1.1 DNS Cache Snooping

- 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

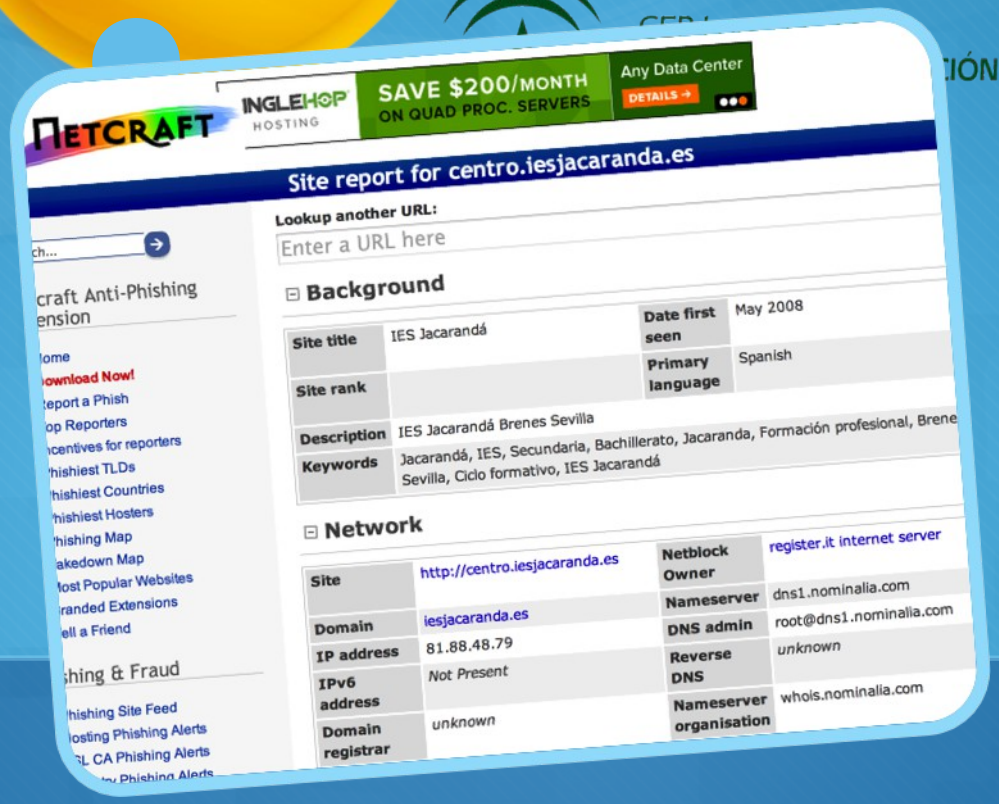
- Una vez obtenidos los objetivos con sus correspondientes Ips habría que situarlos en la red y posicionarlos geográficamente.
- Aplicaciones: tracert, visualroute, …

1.1.2 Tracear y posicionar



1.1.3 Whoi

- Cuando una emp
dominio en Internet
serie de datos en
deben estar en una
información que se
- Por defecto esta
pública y cu
consultarla.

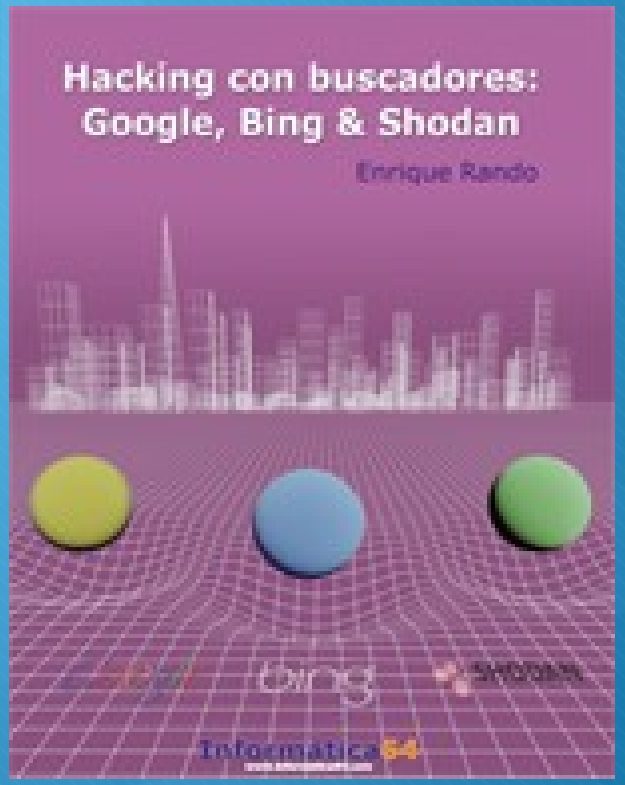


1.1.4 Netcraft

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…

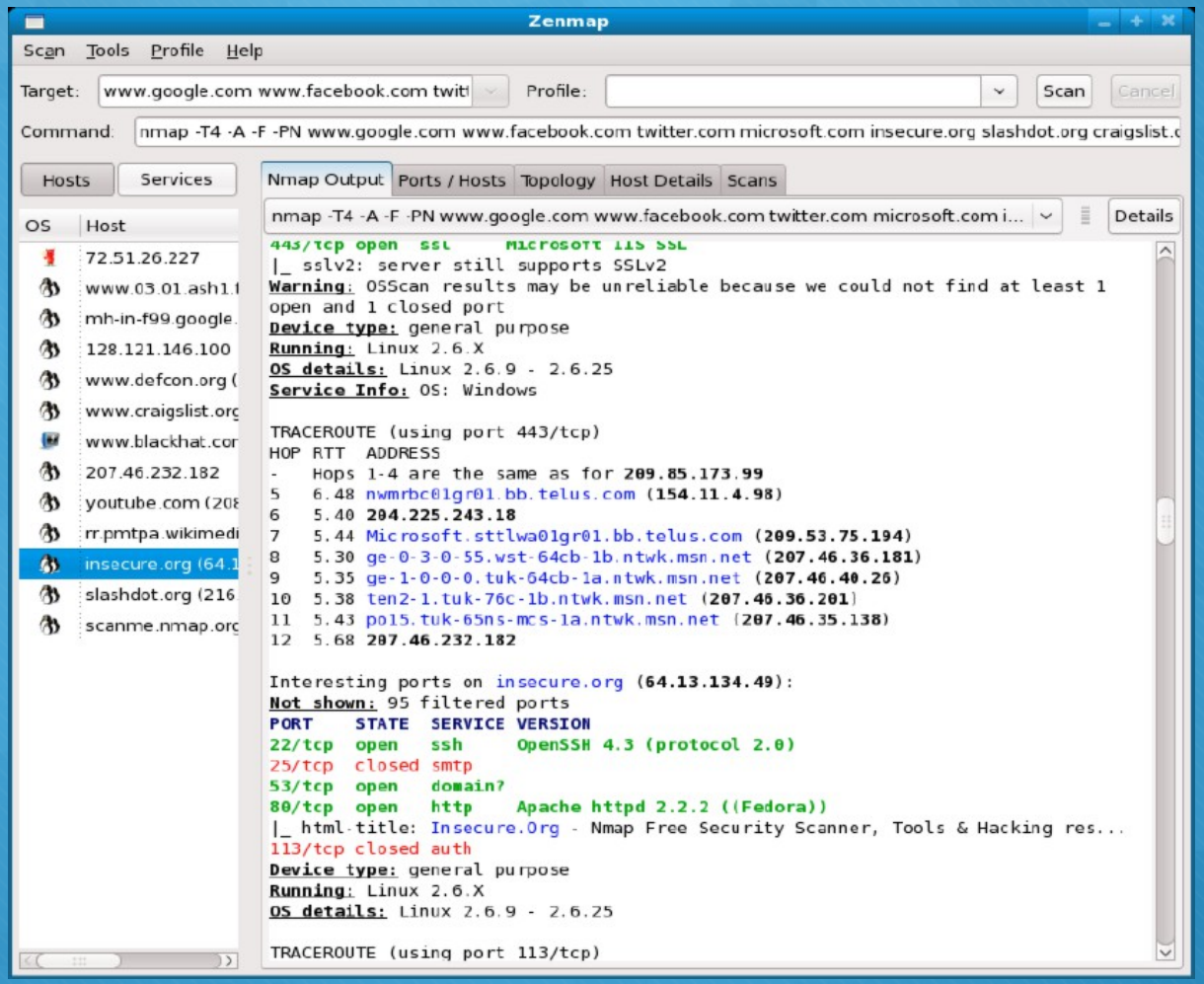
http://www.informatica64.com/foca.aspx

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: www.google.com www.facebook.com twitt
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
nmap -T4 -A -F -PN www.google.com www.facebook.com twitter.com microsoft.com i...
Details
OS
Host
72.51.26.227
www.03.01.ash1.t
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
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 nwmrbc01gr01.bb.telus.com (154.11.4.98)
6 5.40 204.225.243.18
7 5.44 Microsoft.sttlwa01gr01.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)

Zenmap

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-intrusin-i-intelligence-gathering
- http://0xword.com/