

Práctica 5.2: Reconocimiento y recolección de información en fuentes abiertas con buscadores especializados y herramientas automatizadas

Juan Boubeta Puig

Seguridad en los Sistemas Informáticos
Grado en Ingeniería Informática

Curso 2019 – 2020



Índice

- Creación del laboratorio de hacking.
- ¿Qué es el reconocimiento?
- Reconocimiento con Google hacking.
- Reconocimiento con buscadores especializados.
- Clonación de sitios web.
- Reconocimiento DNS.
- Información de directorios Who-Is.
- Búsqueda de bloques de direcciones IP.
- Reconocimiento automatizado con Maltego.
- Rastreo de la ubicación geográfica de un host.
- Rastreo de correos electrónicos.

Creación del laboratorio de hacking (I)

- Descargar e instalar VirtualBox:



The screenshot shows the Oracle VM VirtualBox website. The browser's address bar displays 'virtualbox.org'. The page features the VirtualBox logo on the left and a large 'VirtualBox' title. Below the title, it says 'Welcome to VirtualBox.org!'. The main text describes VirtualBox as a powerful x86 and AMD64/Intel64 virtualization product. A sidebar on the left contains links: About, Screenshots, Downloads, Documentation, End-user docs, Technical docs, Contribute, and Community. At the bottom, a large green button reads 'Download VirtualBox 6.0'.

Oracle VM VirtualBox x +

← → ↺ virtualbox.org



VirtualBox

Welcome to VirtualBox.org!

VirtualBox is a powerful x86 and AMD64/Intel64 [virtualization](#) product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2. See "[About VirtualBox](#)" for an introduction.

Presently, VirtualBox runs on Windows, Linux, Macintosh, and Solaris hosts and supports a large number of [guest operating systems](#) including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and OpenBSD.

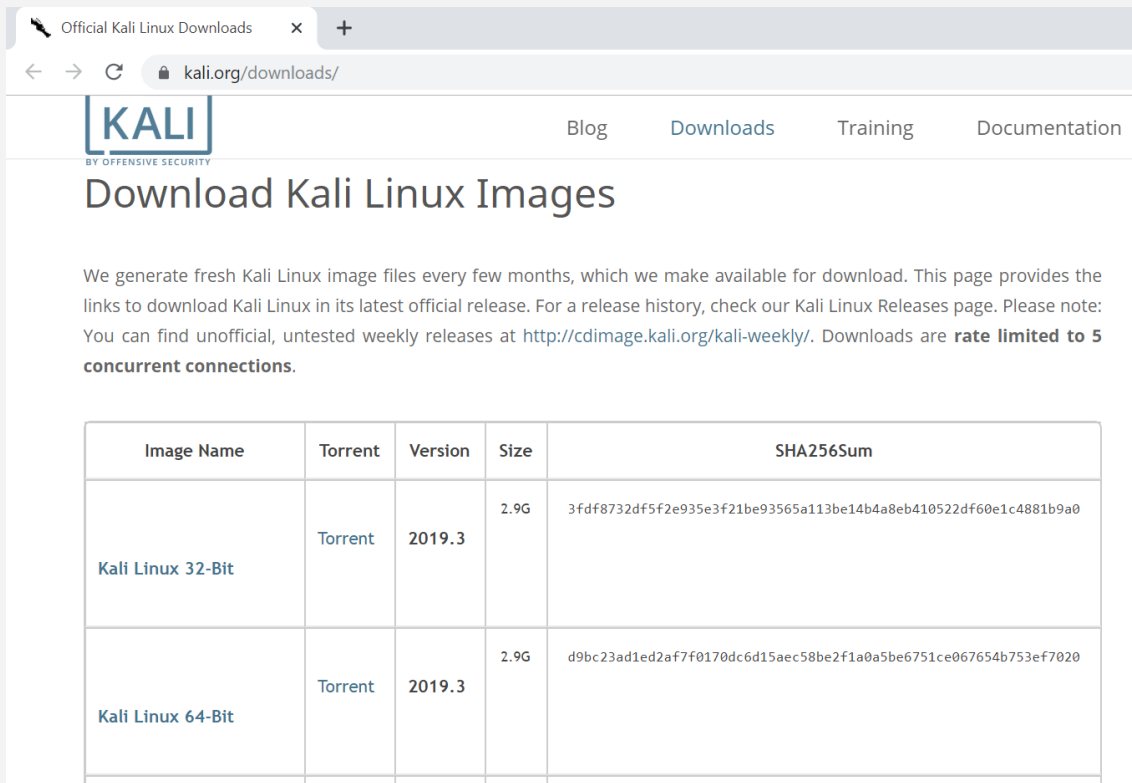
VirtualBox is being actively developed with frequent releases and has an ever growing list of features, supported guest operating systems and platforms it runs on. VirtualBox is a community effort backed by a dedicated company: everyone is encouraged to contribute while Oracle ensures the product always meets professional quality criteria.

[About](#)
[Screenshots](#)
[Downloads](#)
[Documentation](#)
 [End-user docs](#)
 [Technical docs](#)
[Contribute](#)
[Community](#)

Download VirtualBox 6.0

Creación del laboratorio de hacking (II)

- Descargar Kali Linux:



The screenshot shows the 'Official Kali Linux Downloads' page. The browser address bar displays 'kali.org/downloads/'. The page features the Kali Linux logo with the tagline 'BY OFFENSIVE SECURITY'. Navigation links for 'Blog', 'Downloads', 'Training', and 'Documentation' are present. The main heading is 'Download Kali Linux Images'. A paragraph explains that fresh image files are generated every few months and provides links to the latest release and a release history page. It also notes that unofficial weekly releases are available at 'http://cdimage.kali.org/kali-weekly/'. A table lists the available downloads, including 'Kali Linux 32-Bit' and 'Kali Linux 64-Bit', both version 2019.3, with a size of 2.9G. The table also includes the SHA256Sum for each image.

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 32-Bit	Torrent	2019.3	2.9G	3fd8732df5f2e935e3f21be93565a113be14b4a8eb410522df60e1c4881b9a0
Kali Linux 64-Bit	Torrent	2019.3	2.9G	d9bc23ad1ed2af7f0170dc6d15aec58be2f1a0a5be6751ce067654b753ef7020

Creación del laboratorio de hacking (III)

- Crear una máquina virtual en VirtualBox para Kali Linux con las opciones por defecto.
- Se recomienda no usar tildes, espacios ni eñes en la ruta:

← Crear máquina virtual

Nombre y sistema operativo

Seleccione un nombre descriptivo y una carpeta destino para la nueva máquina virtual y seleccione el tipo de sistema operativo que tiene intención de instalar en ella. El nombre que seleccione será usado por VirtualBox para identificar esta máquina.

Nombre:

Carpeta de máquina:

Tipo:


Versión:



Modo experto



Creación del laboratorio de hacking (IV)

Oracle VM VirtualBox Administrador

Archivo Máquina Ayuda

 **Herramientas**

 **Server1**  Apagada

 **Kali Linux 2019-3**  Apagada

General

Nombre: Kali-Linux-2019-3
Sistema operativo: Linux 2.6 / 3.x / 4.x (64-bit)
Ubicación de archivo de preferencias: C:\VirtualBox-maquinas\Kali-Linux-2019-3

Sistema

Memoria base: 1024 MB
Orden de arranque: Disquete, Óptica, Disco duro
Aceleración: VT-x/AMD-V, Paginación anidada, Paravirtualización KVM

Pantalla

Memoria de vídeo: 16 MB
Controlador gráfico: VMSVGA
Servidor de escritorio remoto: Inhabilitado
Grabando: Inhabilitado

Almacenamiento

Controlador: IDE
IDE secundario maestro: [Unidad óptica] Vacío
Controlador: SATA
Puerto SATA 0: Kali-Linux-2019-3.vdi (Normal, 8,00 GB)

Audio

Controlador de anfitrión: Windows DirectSound
Controlador: ICH AC97

Red

Adaptador 1: Intel PRO/1000 MT Desktop (NAT)

USB

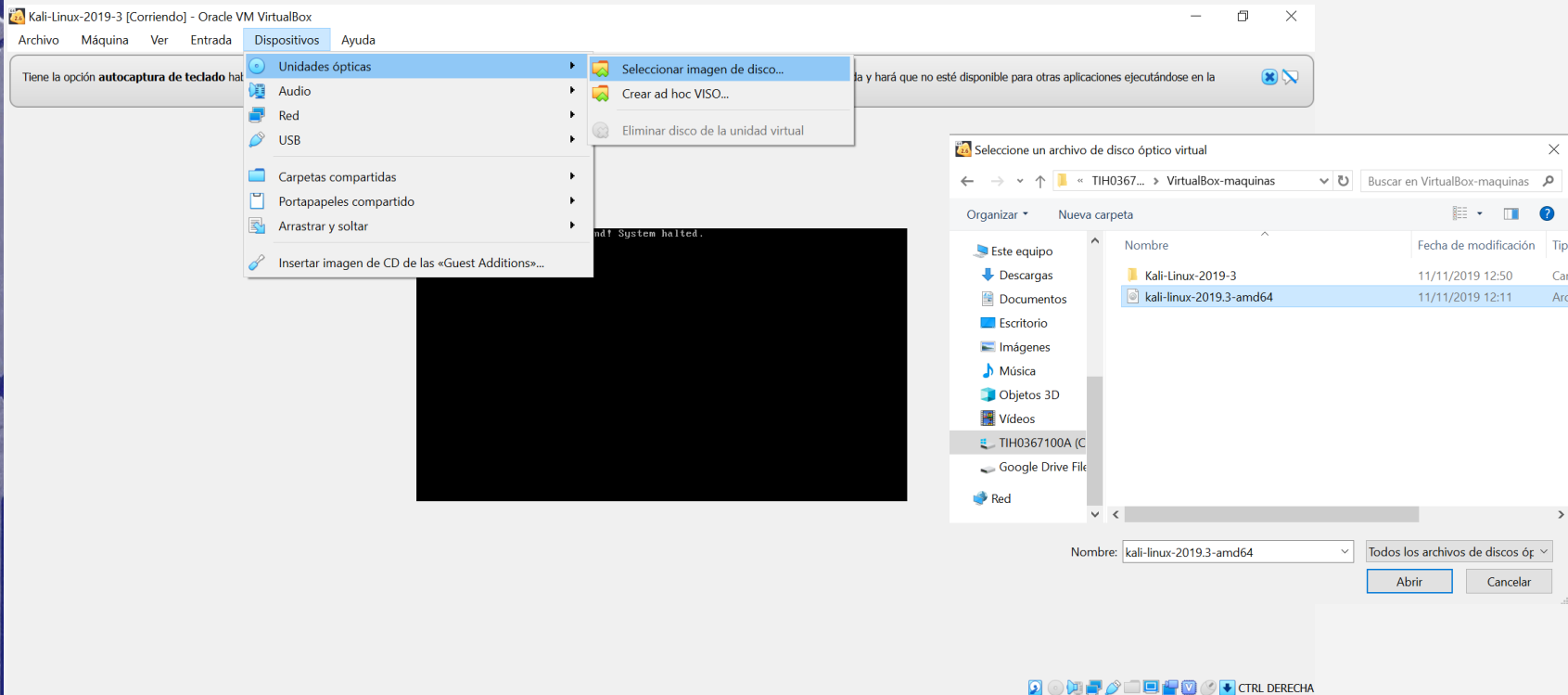
Controlador USB: OHCI
Filtros de dispositivos: 0 (0 activo)

Carpetas compartidas

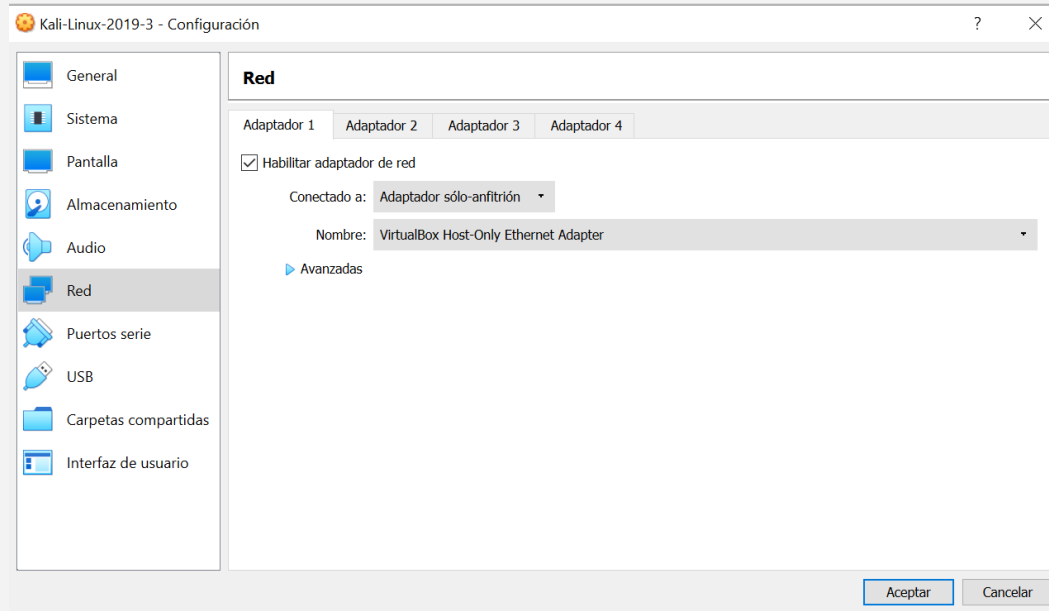
Ninguno

Creación del laboratorio de hacking (V)

- Seleccionar la imagen ISO descargada de Kali Linux:



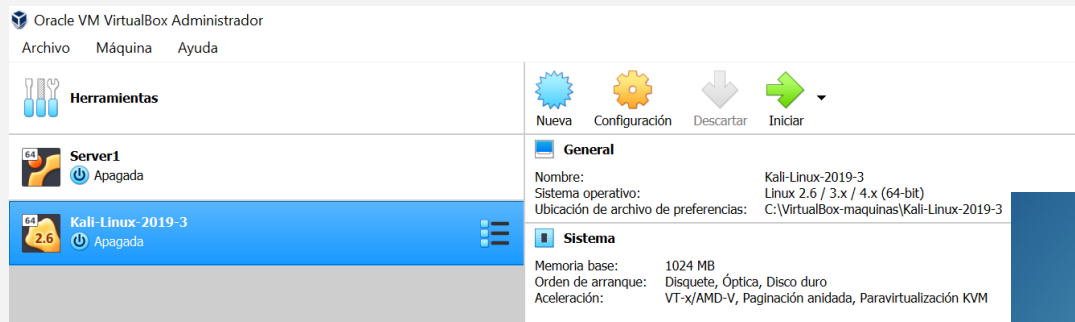
Creación del laboratorio de hacking (VI)



- Otra opción menos segura es usar la conexión en modo puente (*bridge*).

Creación del laboratorio de hacking (VII)

- Ejecutar Kali Linux, a partir de la máquina virtual creada en VirtualBox:





Creación del laboratorio de hacking (VIII)

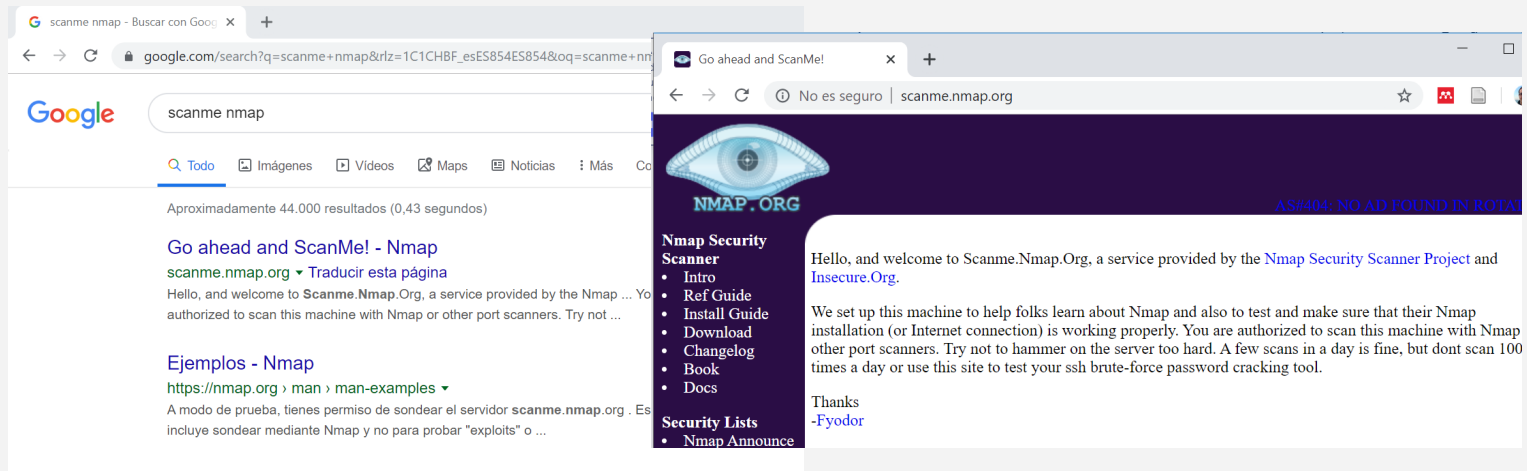
- Usaremos Kali Linux con el siguiente usuario:
 - Usuario: root
 - Contraseña: toor
- ¿Problemas con acceso a Internet? Más información en:
<https://kali.training/topic/configuring-the-network/>

¿Qué es el reconocimiento?

- La primera fase del *pentesting* es el reconocimiento (*footprinting*).
- Consiste en descubrir toda la información relevante de la organización víctima o cliente.
- Existen dos tipos de reconocimiento:
 - **Pasivo:** no tenemos interacción directa con la víctima o el cliente. Por ejemplo, investigación de una empresa a través de Google.
 - **Activo:** existe una interacción directa con la víctima o el objetivo. Por ejemplo, realizar un mapeo de la red, un barrido de ping o la conexión a un puerto de una aplicación.

Reconocimiento con Google hacking

- Reconocimiento con el **buscador genérico** Google realizado en la práctica 5.1 de la asignatura.
- Empresa víctima: *Scanme de Nmap* (sitio mantenido por Fyodor para el que estamos autorizados a realizar pruebas de reconocimiento y escaneo).



Reconocimiento con buscadores especializados (I)

- **Ejercicio 1:** accede a cada uno de los siguientes buscadores especializados, pruébalo e indica cuál es su utilidad:
 - DNSstuff: <https://tools.dnsstuff.com/>
 - DomainTools: <http://whois.domaintools.com>
 - KnowEm: <https://knowem.com/>
 - Namechk: <https://namechk.com/>
 - Pipl: <https://pipl.com/>
 - Robtex: <https://www.robtex.com/>
 - Shodan: <https://www.shodan.io/>



Reconocimiento con buscadores especializados (II)

- Spokeo: <https://www.spokeo.com/>
- TinEye: <https://www.tineye.com/>
- Yasni: <http://www.yasni.com/>

Clonación de sitios web (I)

- Clonamos el sitio web del objetivo para analizarlo posteriormente.
- El clonado también podría servir para realizar ataques de suplantación (*phishing*).
- Para la clonación, usaremos la aplicación HTTTrack, software libre y compatible con Kali Linux.
- Abrir la terminal de Linux e instalar HTTTrack:
 - `sudo apt-get update`
 - `sudo apt-get install httrack`
- Ejecutar HTTTrack en la terminal:
 - `httrack`

Clonación de sitios web (II)

- Como nombre de proyecto indicamos: WebScanTest
- Ruta del *path*: /root/clon
- URL de la web que queremos clonar:
<http://www.webscantest.com>
- Acción: 1 (*Mirror Web Site*)
- *Proxy*: ninguno.
- *Wildcards*: ninguno.
- *Additional options*: ninguno.
- *Ready to launch the mirror?*: Y

Clonación de sitios web (III)

- Una vez finalizado el clonado, aparecerá un mensaje de agradecimiento por el uso de la herramienta:

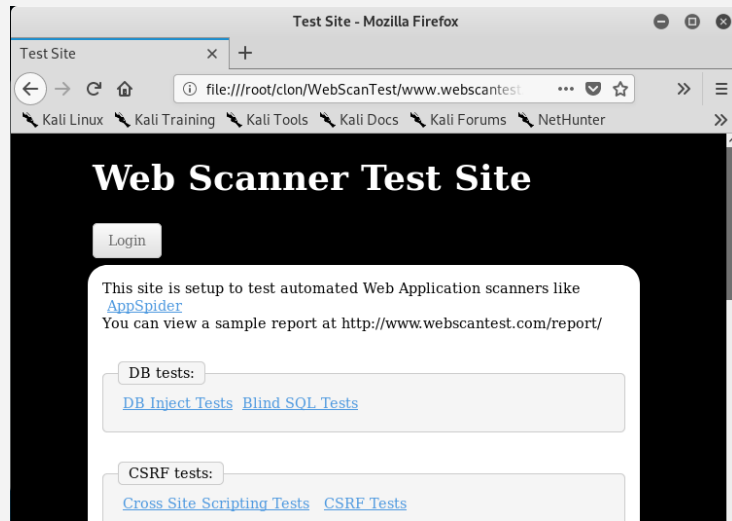
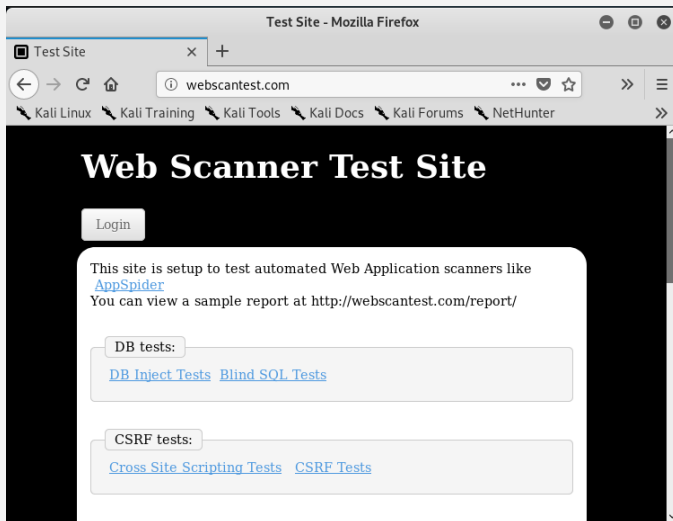
```
File Edit View Search Terminal Help
Ready to launch the mirror? (Y/n) :y

WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Mon, 11 Nov 2019 17:11:03 by HTTrack Website Copier/3.49-2 [XR
&C0'2014]
mirroring http://www.webscantest.com with the wizard help..

* www.webscantest.com/business/account.php?accountId=123456789-abcdef (1381 bytes)
107/123: www.webscantest.com/xmldb/search_by_name.php?index=Lunch (1427 bytes) -
108/124: www.webscantest.com/xmldb/search_by_name.php?index=Waffles (1693 bytes)
* www.webscantest.com/xmldb/search_by_name.php?index=Lunch&action=addtocart&id=10
* www.webscantest.com/xmldb/search_by_name.php?index=Waffles&action=addtocart&id=
* www.webscantest.com/xmldb/search_by_name.php?index=Waffles&action=addtocart&id=
* www.webscantest.com/xmldb/search_by_name.php?index=Waffles&action=addtocart&id=
112/127: www.webscantest.com/business/quantity.php?quantity=1000 (1387 bytes) - 0
114/127: www.webscantest.com/business/access.php?serviceid=123456789 (1370 bytes)
115/127: www.webscantest.com/business/account.php?accountId=123456789-abcdef (138
116/127: www.webscantest.com/csrf/session.php?jsession=123456789 (1297 bytes) - 0
119/127: www.webscantest.com/angular/angular1/styles/bootstrap.css (185901 bytes)
123/127: www.webscantest.com/xmldb/search_by_name.php?index=Lunch&action=addtocar
124/127: www.webscantest.com/xmldb/search_by_name.php?index=Waffles&action=addtoc
125/127: www.webscantest.com/xmldb/search_by_name.php?index=Waffles&action=addtoc
126/127: www.webscantest.com/xmldb/search_by_name.php?index=Waffles&action=addtoc
Done.d=1002 (1760 bytes) - OK
Thanks for using HTTrack!
*
```

Clonación de sitios web (IV)

- Comprobamos que el sitio se ha clonado correctamente, accediendo al index.html:
 - Abrir navegador Firefox.
 - File > Open File > /root/clon/WebScanTest/index.html



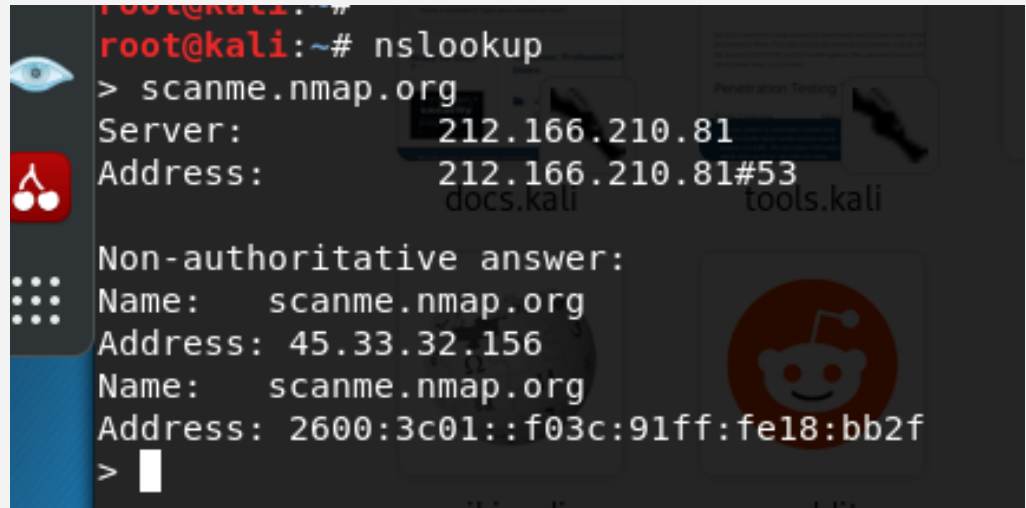
Clonación de sitios web (V)

- **Ejercicio 2:**

- Indica algunas URL de host contenidas en los ficheros del **directorio** /root/clon/WebScanTest/www.webscantest.com
- Busca alguna dirección de correo electrónico que se encuentre en esos ficheros.
- ¿Qué otro tipo de información valiosa se puede obtener del sitio clonado?

Reconocimiento DNS (I)

- Tras conocer el sitio principal de nuestro cliente, podemos hacer una consulta *Domain Name System* (DNS) para conocer su dirección IP.
- Para ello, usamos el comando *nslookup* y le pasamos el sitio scanme.nmap.org

A terminal window on a Kali Linux system showing the output of the 'nslookup scanme.nmap.org' command. The terminal has a dark background with a sidebar on the left containing icons for a blue eye, a red person icon, and a grid of dots. The command prompt is 'root@kali:~#'. The output shows two IP addresses: 212.166.210.81 and 212.166.210.81#53. Below this, it says 'Non-authoritative answer:' and lists two more IP addresses: 45.33.32.156 and 2600:3c01::f03c:91ff:fe18:bb2f. The prompt is currently '>' with a cursor.

```
root@kali:~# nslookup
> scanme.nmap.org
Server:         212.166.210.81
Address:        212.166.210.81#53

Non-authoritative answer:
Name:   scanme.nmap.org
Address: 45.33.32.156
Name:   scanme.nmap.org
Address: 2600:3c01::f03c:91ff:fe18:bb2f
>
```

Reconocimiento DNS (II)

- **Ejercicio 3:**

- ¿Cuántas direcciones IP tiene este sitio?
- Accede al manual del comando con *man nslookup*:
 - ¿Qué opción podemos utilizar para que nos devuelva información sobre los servidores de nombres para el dominio objetivo? ¿Qué empresa provee el DNS nmap.org?
 - ¿Qué opción podemos utilizar para que nos devuelva los servidores de correo para ese dominio? ¿Qué empresa provee el servicio de correo?

- **Ejercicio 4:** repite los mismos pasos del Ejercicio 3 pero para el dominio de la UCA.

Información de directorios Who-Is (I)

- El siguiente paso es obtener información consultando Who-Is.
- Who-Is es una base de datos pública que gestiona información sobre la propiedad de un nombre de dominio o dirección IP.
- Está gestionado por la corporación de Internet para la asignación de nombres y números (ICANN).
- Los Registros de Internet Regionales (RIR) son organizaciones sin ánimos de lucro que administran el espacio de direcciones IP: ARIN, APNIC, AFRINIC, LACNIC y RIPE (https://icannwiki.org/Regional_Internet_Registry).

Información de directorios Who-Is (II)

- Buscamos el nombre de la organización Facebook en <http://whois.arin.net>

The screenshot shows a web browser window with the URL `whois.arin.net/ui/query.do`. The page features the ARIN logo (American Registry for Internet Numbers) and a search bar labeled "SEARCH WhoisRWS" with a note "all requests subject to terms of use". A sidebar on the left contains an "ARIN Online" button. The main content area is titled "WHOIS-RWS" and displays the search results for "Facebook".

You searched for: **Facebook**

Customers
FACEBOOK (C02001848)
Facebook (C02107106)
Facebook (C02107153)
Facebook (C02738182)
FACEBOOK (C03029402)
Facebook (C06910775)
Facebook (C07049343)

On the right side, there is a "RELEVANT LINKS" section with the following links:

- ARIN Whois/Whois-Terms of Service
- Report Whois Inacc
- Search ARIN Whois RDAP

Información de directorios Who-Is (III)

- **Ejercicio 5:**

- Analiza los resultados obtenidos en <http://whois.arin.net> para la empresa Facebook y contesta a las siguientes preguntas:
 - ¿Cuál es la ubicación física de la empresa?
 - ¿Cuándo se registró el nombre del dominio por primera vez?
 - ¿Cuáles son los bloques de direcciones IP asignados a Facebook?
 - La publicación del rango de las IP de la empresa, ¿podría suponer un riesgo de seguridad? ¿Se podría mantener de forma privada esta información, evitando que se publique en Who-Is?

Información de directorios Who-Is (IV)

- **Ejercicio 6:**

- Elige un dominio español y analiza los resultados obtenidos en el NIC (*Network Information Center*) de España
<https://www.nic.es/sgnd/dominio/publicInformacionDominios.action>:
 - ¿Qué tipo de información valiosa nos devuelve la consulta?
 - ¿Se podría utilizar esta información con algún fin malicioso?

Búsqueda de bloques de direcciones IP (I)

- Podemos buscar bloques de direcciones IPv4 e IPv6 de una organización mediante:
 - IPv4Info: <http://ipv4info.com/>
 - Hurricane Electric: <https://bgp.he.net/>

IPv4Info - 212.128.109.1 ip address

No es seguro | [ip4info.com/ip-address/sc648d2/212.128.109.1.html/lamoncloa.gob.es/#](#)

IPv4Info FOR SALE Tools API Store Statistics Search: (domain, ip, ASN or company name)

Your ip: 217.216.29.66 | ONO | AS5739 | Spain | Details... | Login | 198

Ad closed by Google

Report this ad Why this ad? >

Domain **lamoncloa.gob.es** is located on IP address **212.128.109.1** >>

Block start	212.128.96.0
End of block	212.128.127.255
Block size	8192 Domains in block
Block name	SEAP-AGE
AS number	200521
Parent block	212.128.0.0 - 212.128.255.255
Organization	Secretaría de Estado de Administraciones Públicas
City	Madrid
Region/State	Madrid, Comunidad de
Country	ES - Spain
Host name	no record in reverse zone
Domain count	>= 2 Servers around
Domains	1 lamoncloa.gob.es 2 www.lamoncloa.gob.es

Map showing location of Madrid, Spain.

AS200521 Secretaria de Estado de Administraciones Públicas

[bgp.he.net/AS200521#_prefixes](#)

HURRICANE ELECTRIC
INTERNET SERVICES

AS200521 Secretaria de Estado de Administraciones Públicas

Quick Links

- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Exchange Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contact Us

Prefix	Description
91.216.12.0/24	Secretaria de Estado de Administraciones Públicas
93.188.48.0/22	Secretaria de Estado de Administraciones Públicas
93.188.52.0/22	CP-ATOCHA
185.73.172.0/24	Secretaria de Estado de Administraciones Públicas
185.73.174.0/24	Secretaria de Estado de Administraciones Públicas
192.148.208.0/24	Secretaria de Estado de Administraciones Públicas
192.148.209.0/24	Secretaria de Estado de Administraciones Públicas
192.148.210.0/24	Secretaria de Estado de Administraciones Públicas
192.148.211.0/24	Secretaria de Estado de Administraciones Públicas
192.148.212.0/24	Secretaria de Estado de Administraciones Públicas
192.148.213.0/24	Secretaria de Estado de Administraciones Públicas
192.148.215.0/24	Secretaria de Estado de Administraciones Públicas
192.187.18.0/24	Secretaria de Estado de Administraciones Públicas

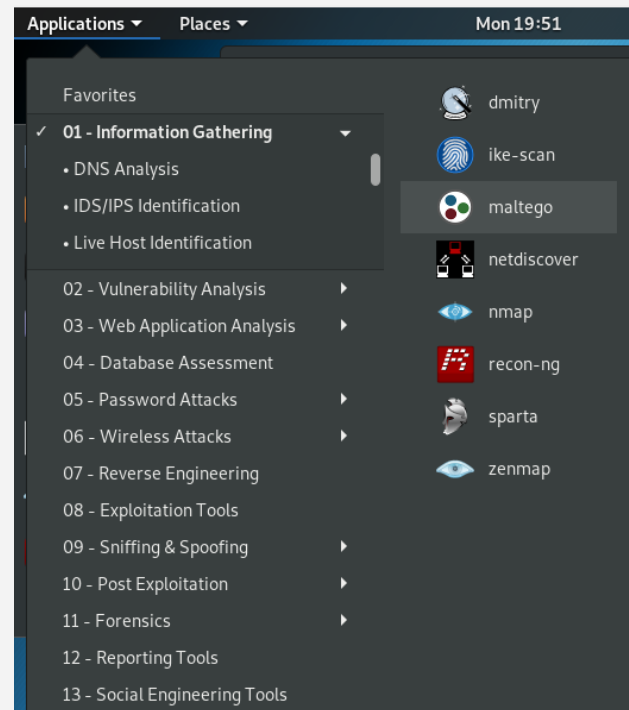
Búsqueda de bloques de direcciones IP (II)

- **Ejercicio 7:**

- Busca el dominio de la Presidencia de España (lamoncloa.gob.es) en <http://ipv4info.com/> y <https://bgp.he.net/>
- ¿Qué información relevante podemos obtener en cada web?

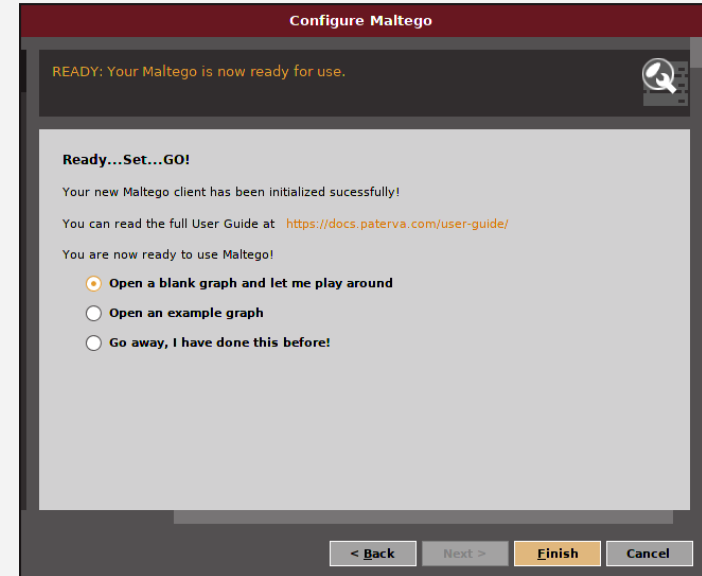
Reconocimiento automatizado con Maltego (I)

- Para realizar un reconocimiento automatizado y más eficiente utilizaremos la herramienta Maltego.
- Para ejecutarla, accedemos al menú *Applications > Information Gathering > Maltego* de Kali Linux.
- Seleccionamos la opción *Maltego CE*, que es la versión *Community Edition*.
- Debemos registrarnos en Paterva, la empresa creadora de Maltego.



Reconocimiento automatizado con Maltego (II)

- Creamos un gráfico en blanco para probar las transformaciones proporcionadas por Maltego.
- Una transformación es una operación que se aplica sobre un objeto para obtener información adicional.
- Esta información se representa en una estructura de tipo árbol.
- Expandimos el menú *Infrastructure* y arrastramos un objeto de tipo *Domain* al nuevo gráfico.



Reconocimiento automatizado con Maltego (III)

- **Ejercicio 8:**

- Cambiamos el dominio del objeto por google.com
- Hacemos clic derecho sobre el objeto del dominio de Google y seleccionamos *DNS from Domain -> Run All* para que se ejecuten todas las transformaciones del protocolo DNS.
- Obtendremos un gráfico de árbol con los hosts que forman parte del dominio de Google.
- Sobre una de las máquinas, aplicamos la transformación de resolución de direcciones IP. ¿Qué información se obtiene?
- Busca información adicional sobre Maltego en www.paterva.com y aplica otros dos tipos de transformaciones al dominio de Google e indica qué información valiosa se obtiene.



Reconocimiento automatizado con Maltego (IV)

- **Ejercicio 9:**
 - Repite los pasos del Ejercicio 8 usando como dominio el de la UCA.

Rastreo de la ubicación geográfica de un host

- A partir de un objetivo concreto (host descubierto), investigaremos cuál es su ubicación geográfica.
- Usaremos la aplicación web: <http://en.dnstools.ch/visual-traceroute.html>
- **Ejercicio 10:**
 - ¿Qué información obtenemos para el dominio Google?
 - ¿Y para Facebook?

Traceroute on a map - Network- x +

← → ↻ No es seguro | en.dnstools.ch/visual-traceroute.html

Deutsche Version

DNSTools

Home
My IP
Traceroute
Ping
DNS Query
Port Scan
Reverse IP
Dropped Domains

Traceroute on a map About

Traceroute determines which IP-Router the data packets take to get to the target computer. However, traceroute does not always show the actual route. The result may be influenced by firewalls, flawed implementation of IP-stacks, Network Address Translation and IP tunnels.

Parallel to the traceroute query, locations of the nodes are also determined and represented on the map.

Host (Domain/IP)
microsoft.com or bluewin.ch

Intuitive monitoring
PRTG turns data into knowledge. With smart dashboards and reliable notifications.

© 2019 by **secpoint**

Your IP address
IP: 217.218.29.66
Location
Spain
Operating system
Windows
Browser
Chrome

Terminal — bash

```
guest@dnstools.ch:~$ traceroute google.com
1 static.1.241.243.136.clients.your-server.de (136.243.241.1) 0.223 ms
2 core24.fsn1.hetzner.com (213.239.229.53) 0.222 ms
3 core0.fra.hetzner.com (213.239.252.41) 4.842 ms
```



Rastreo de correos electrónicos

- Existen herramientas de análisis de correo que permiten verificar cuál es la IP origen de un email y si el remitente es quien dice ser.
- Un ejemplo es eMailTrackerPro:
<http://www.emailtrackerpro.com/>

Bibliografía

- K. Astudillo B. Hacking Ético: Cómo Convertirse en Hacker Ético en 21 Días o Menos, 3ª edición. ISBN 978-84-9964-767-8. Ra-Ma, 2018.
- M. Á. Caballero Velasco y D. C. Serrano. El Libro del Hacker. ISBN 978-84-415-3964-8. Anaya Multimedia, 2018.
- P. González, G. Sánchez y J. M. Soriano. Pentesting con Kali Linux Rolling Release 2017, 2ª edición. ISBN 978-84-697-6035-2. 0xWORD, 2017.
- R. Hertzog, J. O’Gorman y M. Aharoni. Kali Linux Revealed: Mastering the Penetration Testing Distribution. ISBN 978-0-9976156-0-9. Offsec Press, 2017.

