

esgeeks.com

Footprinting de Sitios Web (Guía del Principiante) - EsGeeks

Hacking · 5 Minutos de lectura

7-9 minutos

Como ya sabemos, hay muchos tipos de footprinting y hoy vamos a hablar sobre footprinting de DNS, sitios web y whois.

En nuestro artículo anterior hemos discutido una **breve introducción de footprinting** para la recopilación de información relacionada con una persona específica. Ahora vamos a conocer algunos otros tipos, con ejemplos prácticos.

Antes que nada, veamos lo que la navegación por un sitio web “objetivo” nos puede proporcionar:

- Software utilizado y su versión
- Detalles del sistema operativo
- Subdominios
- Nombre de un archivo y ruta del archivo
- Plataforma de secuencias de comandos y detalles de un CMS
- Detalles de contacto
- Mucho más.

Empecemos!

1. Footprinting de Whois

Echemos un vistazo rápido a su definición:

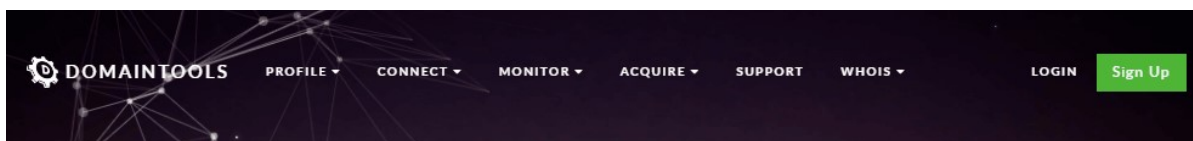
WHOIS es un protocolo de consulta y respuesta que se utiliza para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en Internet y **footprinting** con **whois** es un método para ver información sobre la propiedad de un nombre de dominio como por ejemplo:

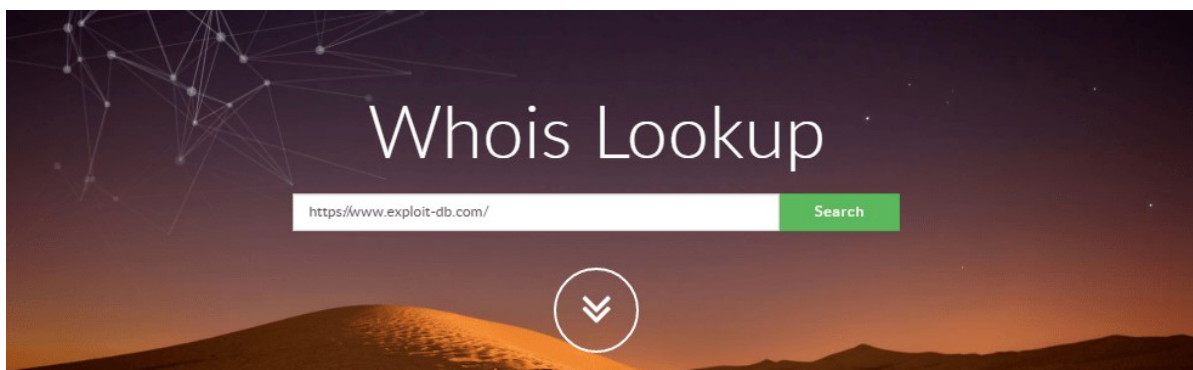
- Detalles del nombre de dominio
- Los datos de contacto (que contienen número de teléfono)
- Dirección de correo electrónico del propietario
- Fecha de registro del nombre de dominio
- Fecha de expiración del nombre de dominio
- Servidores de nombres de dominio

1.1. Búsqueda Whois: DomainTools

Si bien se utiliza ampliamente para consultas de bases de datos que almacenan a los usuarios registrados de un recurso de Internet, como un nombre de dominio, un bloque de direcciones IP o un sistema autónomo, también se utiliza para una gama más amplia de otra información. El protocolo almacena y entrega el contenido de la base de datos en un formato legible por humanos.

- Vaya a la URL <http://whois.domaintools.com/> en su navegador y escriba cualquier nombre de dominio. Por ejemplo: usaré [Exploit-DB](#) (Un sitio web que me gustaría que conocieran)





Whois Domaintools

Ahora usted puede ver que ha creado un registro whois para Exploit-DB donde contiene detalles como: **email, IP, Registrant Org, Name Serves**, entre otros. Bueno, este sitio tiene registro privado con No-IP, pero sirve para ejemplo práctico de lo que podamos conseguir 😊

DOMAINTOOLS	PROFILE ▾	CONNECT ▾	MONITOR ▾	ACQUIRE ▾	SUPPORT	Whois Lookup
— Whois & Quick Stats						
Email	b99062ff0cde4e9b-4...@privacy.no-ip.com abuse@noip.com is associated with ~33,811 domains					↗
Registrant Org	Registration Privacy, No-IP.com is associated with ~11,938 other domains					↗
Registrar	Vitalwerks Internet Solutions LLC DBA No-IP					
Registrar Status	clientTransferProhibited					
Dates	Created on 2009-11-19 - Expires on 2019-11-19 - Updated on 2012-02-22					↗
Name Server(s)	NS1.NO-IP.COM (has 67,366 domains) NS2.NO-IP.COM (has 67,366 domains) NS3.NO-IP.COM (has 67,366 domains) NS4.NO-IP.COM (has 67,366 domains) NS5.NO-IP.COM (has 67,366 domains)					↗
IP Address	192.124.249.8 - 450 other sites hosted on this server					↗
IP Location	🇺🇸 - California - Menifee - Sucuri					
ASN	🇺🇸 AS30148 SUCURI-SEC - Sucuri. US (registered Feb 13, 2015)					

Whois Domaintools: Quick Stats

Hay tantas otras herramientas de uso para **footprint de whois**, por ejemplo:

- [Whois Analyzer pro](#)
- [Caller IP](#)

- [Whois lookup multiple address](#)

2. Footprinting de DNS

Un atacante realiza Footprinting de DNS para enumerar los detalles del registro DNS y el tipo de servidores. Hay 10 tipos de registros DNS que proporcionan información importante relacionada con la ubicación de destino.

- A/AAAA
- SVR
- NS
- TXT
- MX
- CNAME
- SOA
- RP
- PTR
- HINFO

2.1. Herramientas Footprinting de DNS

- [Domain Dossier](#) es una herramienta completa en línea para Footprinting de DNS, así como también para footprint de whois.

Utilizando domain dossier, éste verificará los registros DNS de Exploit-DB, seleccione la casilla de verificación para **DNS records** y **traceroute** y luego haga clic en Go.

Domain Dossier Investigate domains and IP addresses

domain or IP address

☐ domain whois record
 ☐ DNS records
 ☐ traceroute

☐ network whois record
 ☐ service scan

user: anonymous [190.233.89.64]
 balance: 49 units
[log in](#) | [account info](#)

CentralOps.net

Web de Domain Dossier

Puede observar que, los datos que hemos recibido de domain dossier es parecido al que anteriormente vimos con whois e incluye detalles de los registros DNS: **TXT, SOA, NS, MX, A y PTR.**

Address lookup

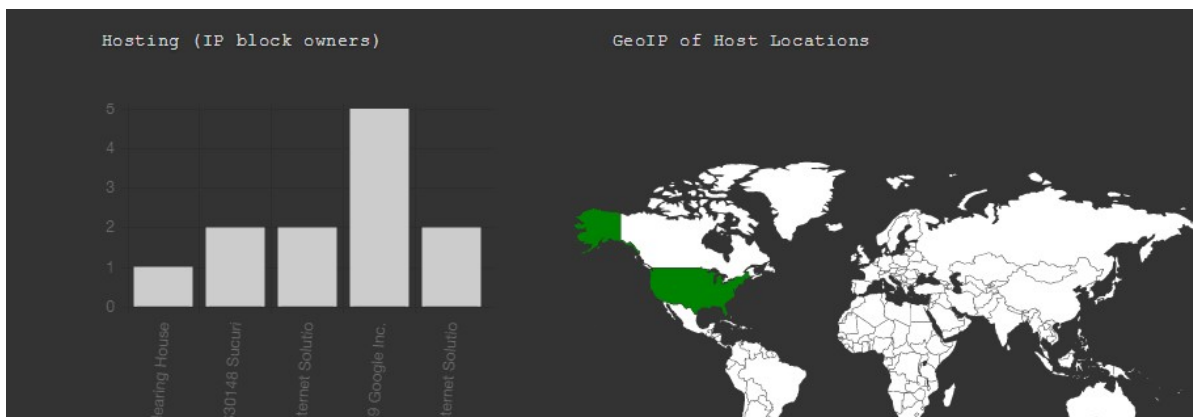
canonical name www.exploit-db.com.
 aliases
 addresses **192.124.249.8**

DNS records

name	class	type	data	time to live
www.exploit-db.com	IN	A	192.124.249.8	60s (00:01:00)
exploit-db.com	IN	SOA	server: ns2.no-ip.com email: hostmaster@no-ip.com serial: 2009111962 refresh: 10800 retry: 1800 expire: 604800 minimum ttl: 1800	86400s (1.00:00:00)
exploit-db.com	IN	NS	ns1.no-ip.com	86400s (1.00:00:00)
exploit-db.com	IN	NS	ns2.no-ip.com	86400s (1.00:00:00)
exploit-db.com	IN	NS	ns3.no-ip.com	86400s (1.00:00:00)

Domain Dossier: DNS Records

- [DNS Dumpster](#) también es otra alternativa gratis online para footprinting de DNS. Esta herramienta puede descubrir hosts relacionados con un dominio, recoger 40K de subdominios y presentar los resultados en un XLS para facilitar la referencia.

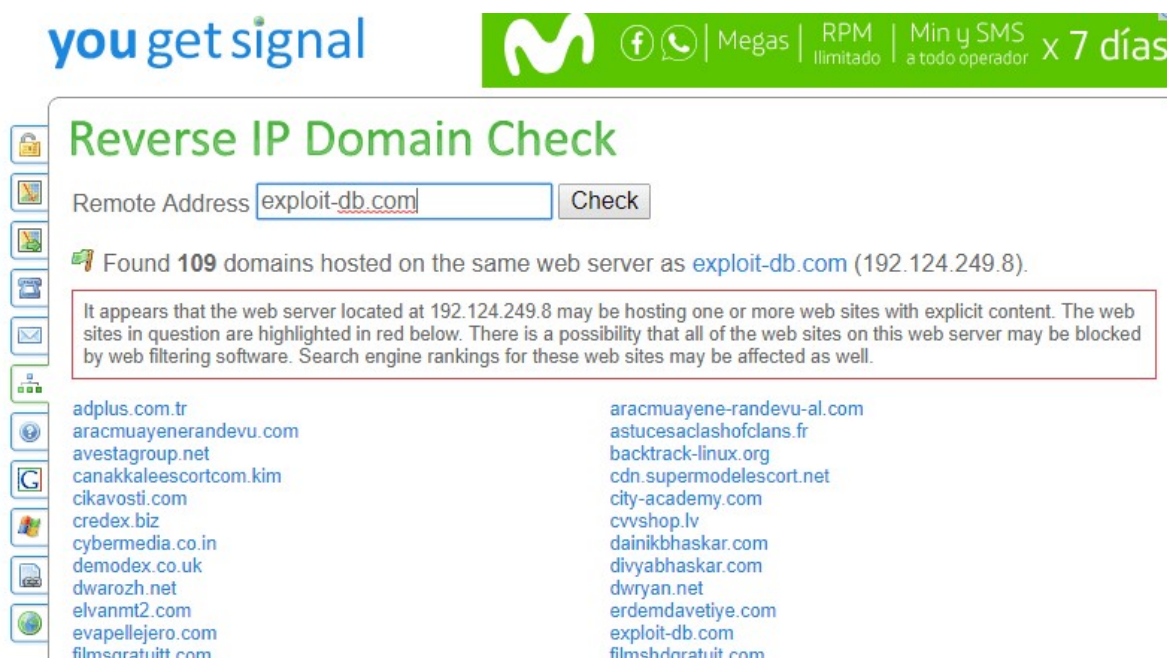




DNS Dumpster

- [You get signal](#) es también una herramienta en línea para el uso de footprinting DNS, así como para footprinting de red.

La opción **Reverse IP Domain Check** toma un nombre de dominio o una dirección IP que apunta a un servidor web y busca otros sitios que, se sabe, están alojados en ese mismo servidor web. Los datos se obtienen de los resultados de los motores de búsqueda y no se garantiza que estén completos.



You Get Signal – Reverse IP Domain Check

3. Footprinting de Sitios Web

El Website Footprinting es una técnica para extraer los detalles relacionados con el sitio web, como por ejemplo:

- ### 3.1. Herramientas de Footprinting de Sitios Web

- Contiene toda la información del pasado hasta el escenario actual de cualquier sitio web ya sea su diseño o contenido de todo lo relacionado con el sitio web. En palabras simples, contiene la historia de cualquier sitio web.

PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.

1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017						
JAN							FEB							MAR							APR						
1	2	3	4	5	6	7	1	2	3	4	1	2	3	4	1												
8	9	10	11	12	13	14	5	6	7	8	9	10	11	5	6	7	8	9	10	11	2	3	4	5	6	7	8

15	16	17	18	19	20	21	12	13	14	15	16	17	18	12	13	14	15	16	17	18	9	10	11	12	13	14	15
22	23	24	25	26	27	28	19	20	21	22	23	24	25	19	20	21	22	23	24	25	16	17	18	19	20	21	22
29	30	31					26	27	28					26	27	28	29	30	31		23	24	25	26	27	28	29
																					30						
MAY							JUN							JUL							AUG						
1	2	3	4	5	6		1	2	3					1							1	2	3	4	5		

Archive.org: Web



- [Built With](#) es otra herramienta en línea que permite detectar técnicas y framework utilizado por algún sitio web.

Esta plataforma incluye información sobre widgets, analytics, frameworks, CMS, anunciantes, redes de distribución de contenido, estándares web, servidores web; por nombrar algunas características.

Tomando como ejemplo de Exploit-DB.org nuevamente, encontramos las siguientes cosas:

EXPLOIT-DB.COM/

Technology Profile

Web Server View Global Trends  nginx nginx Usage Statistics - Download list of all nginx websites ⓘ nginx [engine x] is a HTTP server and mail proxy server written by Igor Sysoev.	Profile Details Last updated 11th August. We know of 60 active technologies on this page and 57 technologies removed from exploit-db.com since 3rd April 2011. Link to this page.
Nameserver Providers View Global Trends  No-ip No-ip Usage Statistics - Download list of all No-ip websites ⓘ Free dynamic dns service.	Access more of BuiltWith Create a free account to see more detailed data, more trends history and try out some of the Pro features of BuiltWith.

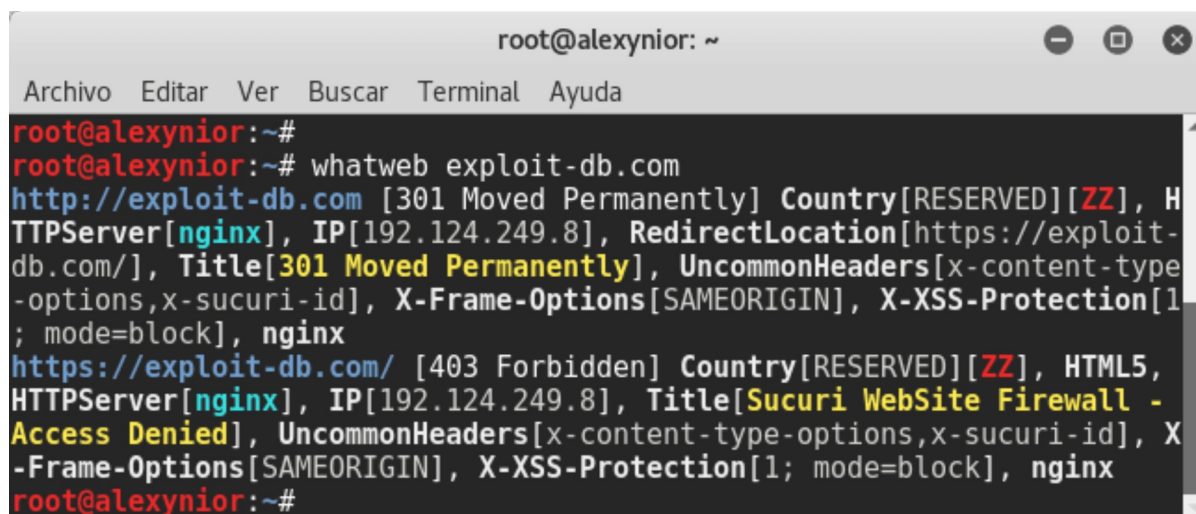
Built With

- **Whatweb** también puede identificar todo tipo de información sobre un sitio web online, como por ejemplo: Plataforma, plataforma CMS, tipo script, Google Analytics, plataforma de servidor web y dirección IP. **Un pentester puede utilizar esta herramienta como un escáner de vulnerabilidades.**

Abra el terminal en kali Linux y escriba el siguiente comando:


```
whatweb www.exploit-db.com
```

Como resultado, recibimos la misma información que la anterior:



```
root@alexynior: ~
Archivo  Editor  Ver  Buscar  Terminal  Ayuda
root@alexynior:~#
root@alexynior:~# whatweb exploit-db.com
http://exploit-db.com [301 Moved Permanently] Country[RESERVED][ZZ], HTTPServer[nginx], IP[192.124.249.8], RedirectLocation[https://exploit-db.com/], Title[301 Moved Permanently], UncommonHeaders[x-content-type-options,x-sucuri-id], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block], nginx
https://exploit-db.com/ [403 Forbidden] Country[RESERVED][ZZ], HTML5, HTTPServer[nginx], IP[192.124.249.8], Title[Sucuri WebSite Firewall - Access Denied], UncommonHeaders[x-content-type-options,x-sucuri-id], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block], nginx
root@alexynior:~#
```

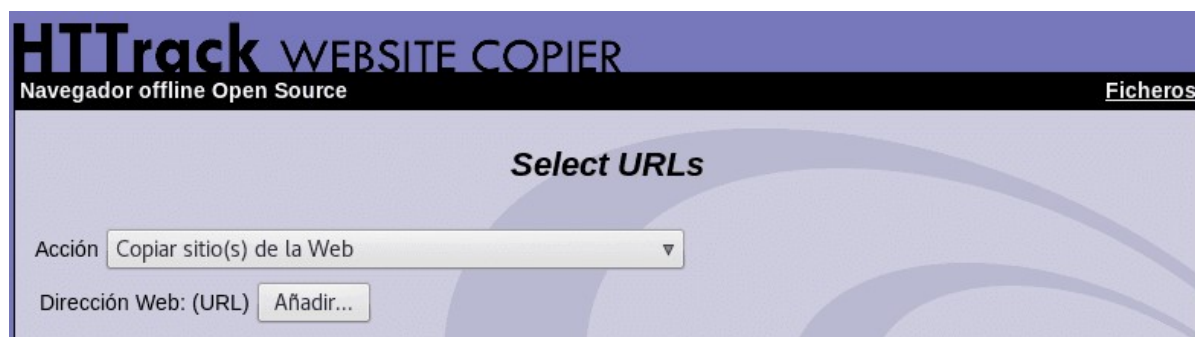
Comando whatweb en Kali Linux

3.2. Web Crawling

Hay muchas herramientas para rastrear un sitio web. A modo de ejemplo revisaremos HTTrack y dejaremos algunas otras opciones.

- [HTTrack](#) es un rastreador web gratuito, de código abierto y navegador offline, desarrollado por Xavier Roche. Le permite descargar un sitio Web desde Internet a un directorio local, crear recursivamente todos los directorios, obtener HTML, imágenes y otros archivos desde el servidor a su computadora. HTTrack organiza la estructura de enlaces relativa del sitio original.

Sólo tiene que proporcionar la URL para comenzar a descargar el sitio web.





HTTrack Website Copier

Otras alternativas para Web Crawling

- [Web Data Extractor Pro](#) es una herramienta de scraping web diseñada específicamente para la recopilación masiva de varios tipos de datos. Puede recolectar direcciones URL, números de teléfono y fax, direcciones de correo electrónico, así como información de meta etiquetas. La característica especial de WDE Pro es la extracción personalizada de datos estructurados.
- [Website-Watcher](#) es una potente y sencilla herramienta de monitorización de sitios web, perfectamente adaptada tanto al usuario principiante como avanzado. Puede descargarlo desde [aquí](#).

Hasta aquí hemos visto una serie de herramientas gratuitas para cada uno de los Footprinting mencionados. Hay muchas más, así que, la que usted conozca y le sea útil por favor comparta con los demás en los comentarios. ¡Y no se olvide de compartir el artículo!

