

PCM | Secretaría de Gobierno
y Transformación Digital

CENTRO NACIONAL DE SEGURIDAD DIGITAL



Ethical Hacking

Ing. Maurice Frayssinet Delgado
mfrayssinet@gmail.com
Tfl. (+51)980.997.203

Unidad 2

Reconocimiento del objetivo



Unidad 2. Reconocimiento del objetivo

- 2.1 Conceptos de Footprinting
- 2.2 Footprinting a través de motores de búsqueda
- 2.3 Footprinting a través de redes sociales
- 2.4 Consultas DNS, WHOIS
- 2.5 Google hacking



2.1 Conceptos de Footprinting

Resumen de la tecnología

- La fase de Footprinting permite al atacante recopilar información sobre la arquitectura interna y externa; él tiene que enfrentar un objetivo.
- La recopilación de información también ayuda a identificar las vulnerabilidades dentro de un sistema, que explota, para obtener acceso.
- Obtener información profunda sobre el objetivo reduce el área de enfoque y acerca al atacante al objetivo.
- El atacante enfoca el objetivo por medio del rango de direcciones IP que tiene que atravesar, para hackear el objetivo o con respecto a la información del dominio o de lo contrario.



Conceptos de Footprinting

El primer paso para hackeo ético es Footprinting.

Footprinting es la recopilación de toda la información posible sobre el objetivo y la red objetivo.

Esta recopilación de información ayuda a identificar diferentes formas posibles de ingresar a la red objetivo.

Esta recopilación de información puede haberse reunido a través de información personal disponible públicamente e información confidencial de cualquier fuente secreta.

Por lo general, la huella y el reconocimiento es realizar ataques de ingeniería social, ataques a sistemas o redes, o mediante cualquier otra técnica.

Los métodos activos y pasivos de reconocimiento también son populares para obtener información del objetivo directa o indirectamente.

El propósito general de esta fase es mantener la interacción con el objetivo para obtener información sin ninguna detección o alerta.

Footprinting seudónima

Footprinting seudónima incluye la huella a través de fuentes en línea. En las huellas seudónimas, la información sobre un objetivo se comparte publicando con un nombre falso.

Este tipo de información se comparte con la credencial real para evitar el rastreo a una fuente real de información.



Footprinting de internet



Footprinting de Internet incluye los métodos de Footprinting y reconocimiento para obtener información a través de Internet. En Internet Footprinting, procesos como Google Hacking, Google Search, Google Application, incluidos motores de búsqueda que no sean Google también.

Principales objetivos de Footprinting

1. Conocer la
postura de
seguridad.

2. Reducir el área de
enfoque.

Principales objetivos de Footprinting

3. Identificar
vulnerabilidades.

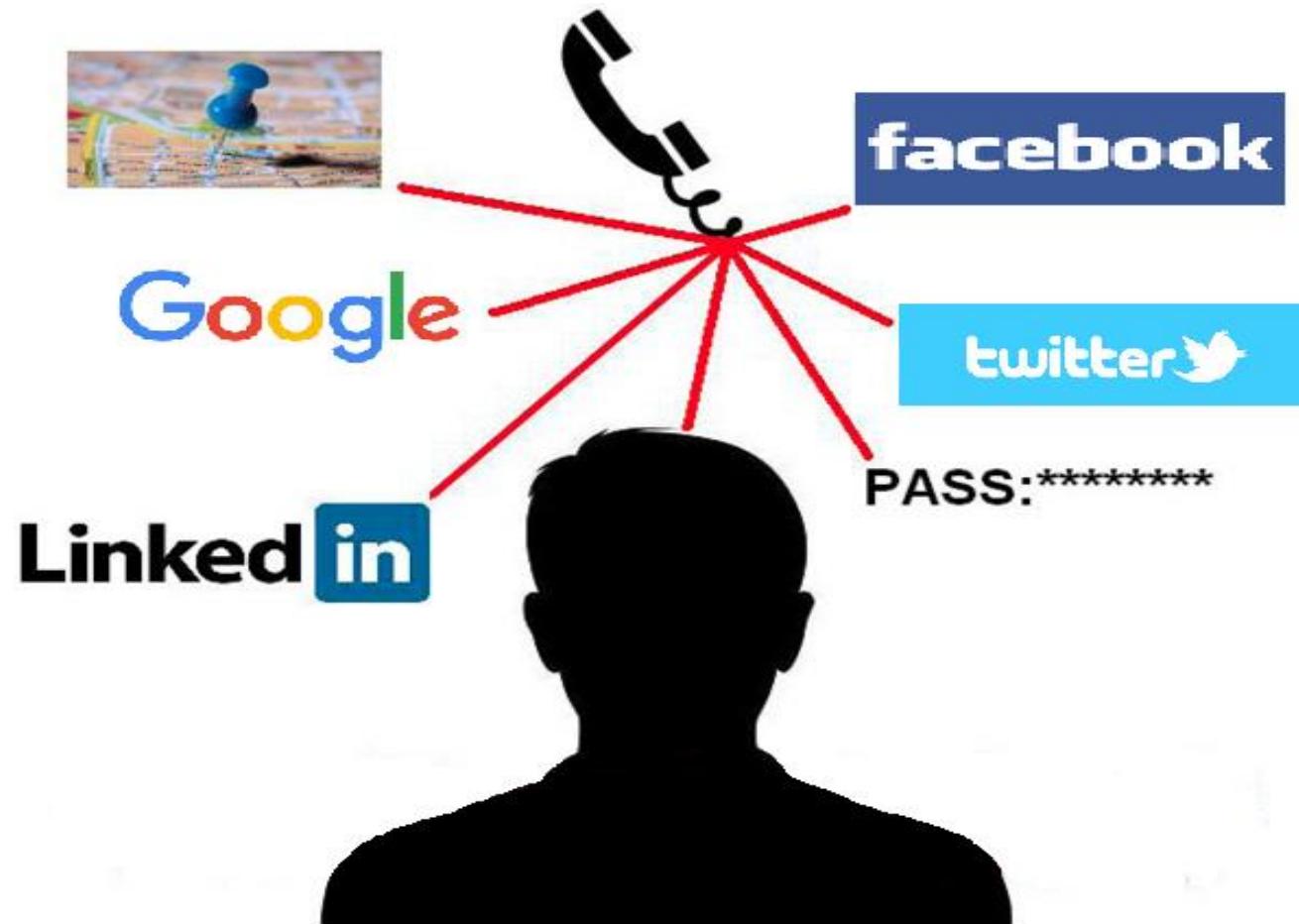
4. Dibujar un mapa
de red.

Metodología de Footprinting

No es gran cosa obtener información sobre nadie, ya que Internet, las redes sociales, los sitios web oficiales y otros recursos tienen mucha información sobre sus usuarios que no es sensible, pero una recopilación de información puede cumplir los requisitos de un atacante y el atacante puede reunir suficiente información por un pequeño esfuerzo.



Metodología de Footprinting



Técnicas más utilizadas por los hackers

1. Footprinting a través de motores de búsqueda.
2. Footprinting a través de técnicas avanzadas de hackeo de Google.
3. Footprinting a través de sitios de redes sociales.



Técnicas más utilizadas por los hackers

4. Footprinting a través de sitios web.
5. Footprinting por correo electrónico.
6. Footprinting a través de la inteligencia competitiva.
7. Footprinting a través de WHOIS.



Técnicas más utilizadas por los hackers

8. Footprinting a través de DNS.
9. Footprinting a través de la red.
10. Footprinting a través de la ingeniería social.



Metodología



2.2 Footprinting a través de motores de búsqueda

Footprinting a través de motores de búsqueda



Footprinting a través de motores de búsqueda

- La opción más básica que también es muy receptiva es Footprinting a través de motores de búsqueda.
- Los motores de búsqueda extraen la información sobre una entidad que ha buscado en internet.
- Puede abrir un navegador web y, a través de cualquier motor de búsqueda como Google o Bing, buscar cualquier organización.
- El resultado recopila toda la información disponible en Internet.



Ejemplo:

Artículo Discusión Leer Editar Ver historial Buscar en Wikipedia

Google

Para otros usos de este término, véase [Google \(desambiguación\)](#).

Google LLC es una compañía principal subsidiaria de la multinacional estadounidense [Alphabet Inc.](#), cuya especialización son los productos y servicios relacionados con Internet, software, dispositivos electrónicos y otras tecnologías. El principal producto de Google es el [motor de búsqueda](#) de contenido en Internet, del mismo nombre, aunque ofrece también otros productos y servicios como la suite ofimática [Google Drive](#), el correo electrónico llamado [Gmail](#), sus servicios de mapas [Google Maps](#), [Google Street View](#) y [Google Earth](#), el sitio web de vídeos [YouTube](#) y otras utilidades web como [Google Libros](#) o [Google Noticias](#), [Google Chrome](#) y la red social [Google+](#) este último sacado fuera de línea en el primer cuatrimestre de 2019. Por otra parte, lidera el desarrollo del sistema operativo basado en [Linux](#), [Android](#), orientado a teléfonos inteligentes, tabletas, televisores y automóviles y en gafas de realidad aumentada, las [Google Glass](#). Su eslogan es «*Do the Right Thing*» («Haz lo correcto»).¹

Con miles de servidores y [centros de datos](#) presentes en todo el mundo, Google es capaz de procesar más de 1000 millones de peticiones de búsqueda diarias y su [motor de búsqueda](#) es el [sitio web](#) más visitado a nivel mundial tal como muestra el ranking web internacional.²

La empresa ha sido criticada por colaborar con determinados países en la censura de Internet con el afán de expandirse comercialmente en ellos y por la infracción reiterada de derechos de autor. También es objeto de críticas por presunta ingeniería fiscal en diferentes países, y por ser una de las empresas que colaboran con las agencias de inteligencia en la [red de vigilancia mundial](#), sacada a la luz en 2013.

[Índice \[mostrar\]](#)

Historia [editar]

Larry Page y Sergey Brin comenzaron Google como un proyecto universitario en enero de 1996 cuando ambos eran estudiantes de posgrado en ciencias de la computación en la [Universidad de Stanford](#). El nombre original del buscador era BackRub, en 1997 los fundadores deciden cambiar el nombre a Google inspirados por el término matemático «gúgol» que se refiere al número 10

Google LLC

Google



Googleplex (oficinas corporativas) en julio de 2016

Tipo	Subsidiaria
ISIN	US02079K3059 y US02079K1079
Industria	Internet Software Hardware Tecnología
Forma legal	sociedad por acciones
Fundación	4 de septiembre de 1998 (21 años)
Fundador	Serguéi Brin y Larry Page

<https://es.wikipedia.org/wiki/Google>

Descripción de ejemplo:

- La búsqueda de google muestra la información sobre el motor de búsqueda más popular del mundo.
- Esta información incluye la ubicación de la sede, la fecha en que se fundó la organización, los nombres de los fundadores, el número de empleados, la organización matriz y su sitio web oficial.
- Puede desplazarse a su sitio web oficial para obtener más información o cualquier otro sitio web para obtener información al respecto.
- Además de esta información disponible públicamente, los sitios web y los cachés de los motores de búsqueda también pueden servir la información que no está disponible, actualizada o modificada en el sitio web oficial.

Encontrar sitios web públicos y restringidos de la empresa

- Durante la recopilación de información, el atacante también recopila información oficial del sitio web de la organización, incluidas sus URL públicas y restringidas.
- El sitio web oficial puede buscar a través de un motor de búsqueda como Google, Bing y otros.
- Para encontrar la URL restringida de una organización, utilizando el método de prueba y error, utilizando diferentes servicios que pueden obtener la información de sitios web como www.netcraft.com.

Ejemplo: Página Web de Netcraft

The screenshot shows the Netcraft homepage with a red header containing the title "Ejemplo: Página Web de Netcraft". Below the header is the Netcraft logo and a navigation bar with links for Services, Solutions, News, Company, Resources, a search bar, Report Fraud, and Request Demo.

Key statistics displayed on the page:

- 83 million phishing sites blocked
- 1.2 billion websites explored
- 25 years keeping networks secure
- 2 Queen's Awards for Enterprise

The page is divided into three main sections:

- Protect your customers from cybercrime**: Features an icon of a laptop with a fishhook. Description: "With our ever-expanding and highly automated range of cybercrime disruption services, we're always ready to respond to online threats targeting your organisation and customers." Call-to-action: "Learn More ➔".
- Keep your network safe**: Features an icon of a padlock with a magnifying glass. Description: "Have your application or network tested by experienced security professionals, ensuring that the risk of a cybercrime attack against your organisation is minimised." Call-to-action: "Learn More ➔".
- Explore the internet's growth**: Features an icon of a network graph. Description: "We have been surveying the web since 1995 and can provide insights into trends and movement patterns on hosting companies, certificate authorities and web technologies." Call-to-action: "Learn More ➔".

<https://www.netcraft.com/>

Recopilar información de ubicación

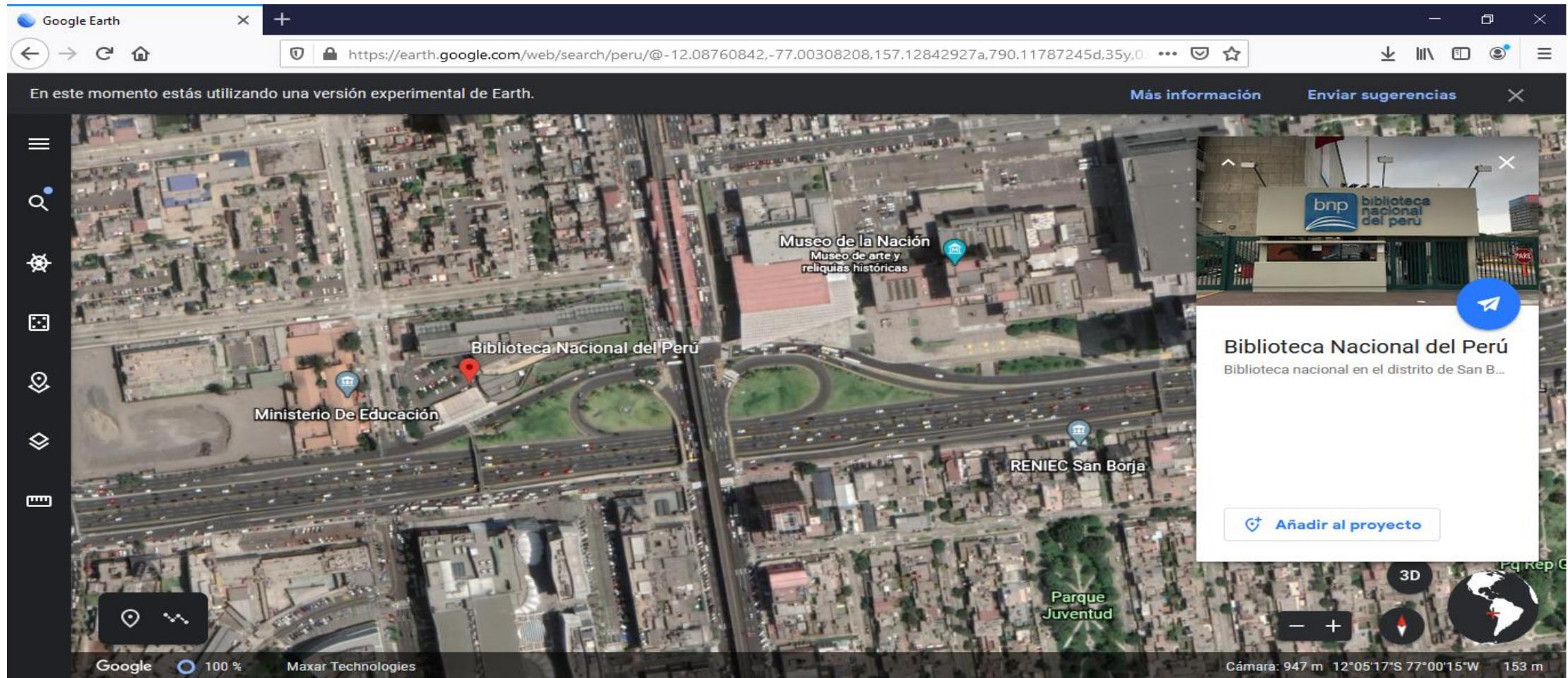
- Después de la recopilación de información básica a través de motores de búsqueda y diferentes servicios como Netcraft y Shodan.
- Puede recopilar información local, como la ubicación física de la sede central con el entorno, la ubicación de las sucursales y otra información relacionada desde la ubicación en línea y los servicios de mapas.

Los servicios en línea más importantes

- Google Earth,
- Mapa de Google,
- Mapa de Bing,
- Wikimapia,
- Mapa de Yahoo,
- Otros servicios de mapa y ubicación.



Ejemplo: Google Earth



<https://earth.google.com/web/>

Servicios de búsqueda en línea de personas

Hay algunos servicios en línea, utilizados popularmente para identificar los números de teléfonos, direcciones y personas.

- ❑ www.privateeye.com
- ❑ www.peoplesearchnow.com
- ❑ www.publicbackgroundchecks.com
- ❑ www.anywho.com
- ❑ www.intelius.com
- ❑ www.4111.com
- ❑ www.peoplefinders.com



Ejemplo: Página Web de Private Eye

Instant People Search

Name Address Reverse Phone

First Name Last Name
City State

Over 2 Billion Records Available!

Reverse Phone Search

Who's calling you? Put in a phone number, and we'll tell you who they are, their address, and other details on the phone number.

Enter the phone number:

Phone Number


People Search

Need to find someone? There are reasons why people want access to information that is on public record. It could be to research family history, genealogy, or to find old college friends and people that you have lost touch with over the years.

PrivateEye.com is your one stop solution for:

- | | |
|---|---------------------|
| ✓ People Search | ✓ Background Checks |
| ✓ Phone Number Look-up | ✓ Criminal Checks |
| ✓ Vital Record Search - Birth, Death, Marriage, And More! | |



Other Available Search Types



- PEOPLE SEARCHES**
Instant People Search
Background Check
Reverse Phone Search



- PUBLIC RECORD SEARCHES**
Criminal Records
Property Records
Bankruptcy



- FAMILY SEARCHES**
Marriage Records

<https://www.privateeye.com/>

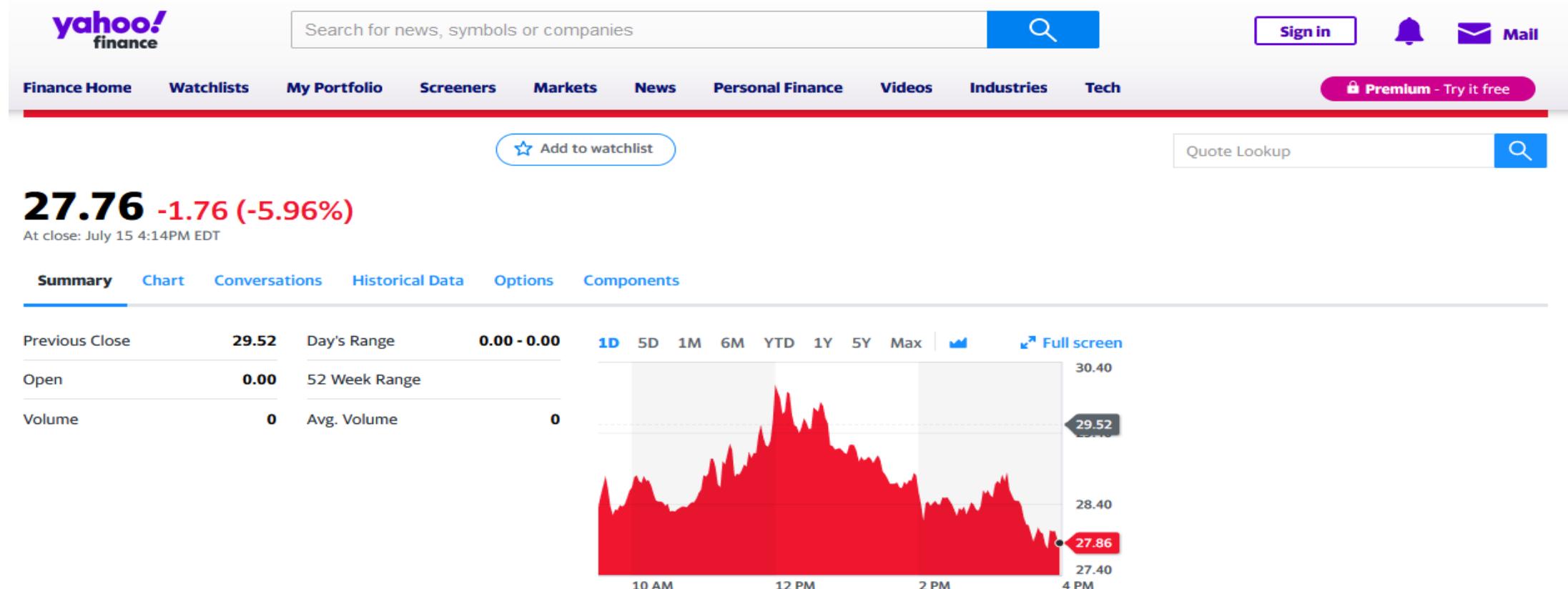
Recopilar información de los servicios financieros

Hay algunos servicios financieros impulsados por diferentes motores de búsqueda que proporcionan información financiera de organizaciones internacionales conocidas. Simplemente buscando su organización objetivo, puede obtener información financiera de estas organizaciones. Google y Yahoo son los servicios financieros en línea más populares.

- [www.google.com / finance](http://www.google.com/finance)
- finance.yahoo.com



Ejemplo: Servicio financiero Yahoo



<https://finance.yahoo.com/>

Footprinting a través de sitios de trabajo

- En los sitios de trabajo, la empresa que ofrece las vacantes a las personas también proporciona la información y el portafolio de su organización.
- Esta información incluye la ubicación de la empresa, información de la industria, información de contacto, número de empleados, requisitos de trabajo, información de hardware y software.
- Del mismo modo, en estos sitios de trabajo, mediante una publicación de trabajo falsa, se puede recopilar información personal de un individuo objetivo.

Algunos de los sitios de trabajo populares

- www.linkedin.com
- www.monster.com
- www.indeed.com
- www.careerbuilder.com



Ejemplo: LinkedIn

The screenshot shows the LinkedIn homepage with a dark header bar. The header includes the LinkedIn logo, navigation links for Inicio, Mi red, Empleos, Mensajes, Notificaciones (with 14 notifications), Yo, Products, and a link to 'Probar Premium gratis durante 1 mes'.

The main content area displays a grid of job posts from different companies:

- Celepsa**: O237 - Practicante de Sistemas. Located in Lima, PE. Posted 1 week ago. 9 antiguos alumnos.
- Bitel Perú**: E-067 | Practicante Profesional de sistemas. Located in Lima, PE. Posted 1 week ago. 19 solicitudes.
- BANCO DE COMERCIO**: Analista de Inteligencia comercial. Located in San Isidro, Lima, Perú. Posted 2 days ago. 2 antiguos empleados.
- IBM**: Service Integration Leader. Located in Lima, PE. Posted 1 day ago. 27 antiguos alumnos.
- Cheil**: IT Support Specialist. Located in Lima, Perú. Posted 2 weeks ago. 1 antiguo alumno.
- Indra**: Recién egresados de Ingeniería de Sistemas, Informática,... Located in Lima, Perú. Posted 3 weeks ago. 1 antiguo empleado.
- (T302)**: (T302) - ADMINISTRADOR I GESTIÓN DE ACCESOS. Located in Lima, PE. Posted 5 days ago. 13 solicitudes.
- Colegio de Notarios de Lima**: [MP57] Auxiliar de Sistemas e Informática. Located in Lima, PE. Posted 1 week ago. 11 solicitudes.

At the bottom right of the page, there are buttons for 'Mensajes' and three dots for more options.

<https://www.linkedin.com/>

Monitoreo de objetivos mediante alertas

Google, Yahoo y otros servicios de alerta ofrecen servicios de monitoreo de contenido con una función de alerta que notifica al suscriptor con la información más reciente y actualizada relacionada con el tema suscrito.



Ejemplo: Servicio de alertas de Google

The screenshot shows the Google Alerts configuration page. At the top, it says "Alertas" and "Supervisa la Web para encontrar nuevos contenidos interesantes". Below that is a search bar containing "seguridad de información". The main area contains six dropdown settings:

- Frecuencia: Como máximo, una vez al día
- Fuentes: Automático
- Idioma: español
- Región: Todas las regiones
- Cantidad: Solo los mejores resultados
- Enviar a: flormeza1691@gmail.com

At the bottom are two buttons: "Actualizar alerta" and "Ocultar opciones ▾".

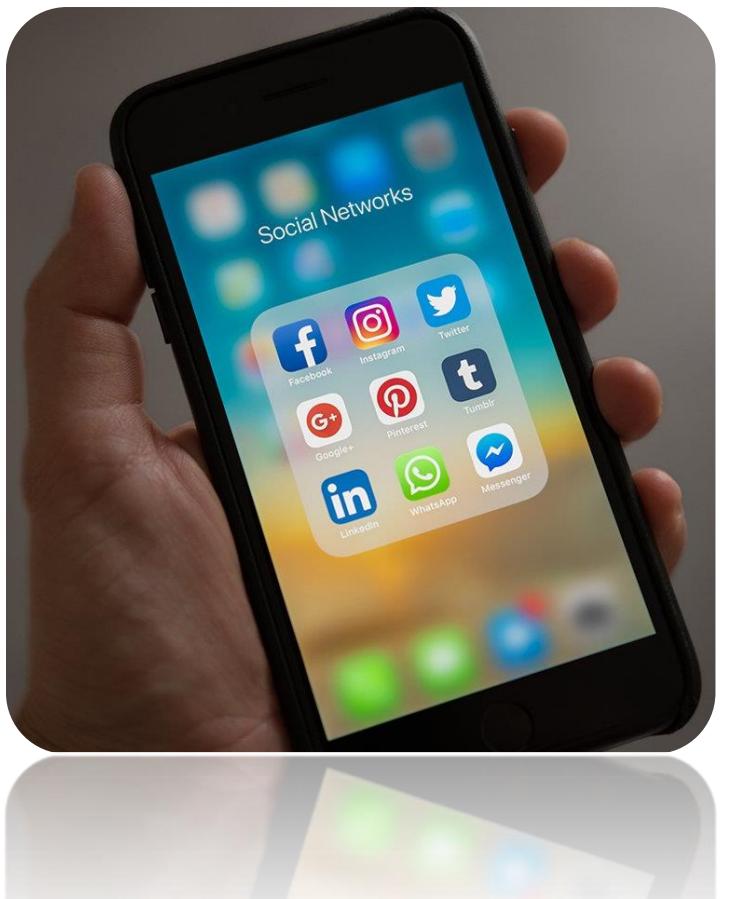
<https://www.google.com/alerts>

Recopilación de información mediante grupos, foros y blogs

- Grupos, foros, blogs y comunidades pueden ser una gran fuente de información confidencial.
- Unirse a una identificación falsa en estas plataformas y llegar más cerca del grupo de la organización objetivo no es un gran problema para nadie.
- Cualquier oficial y un grupo no oficial puede filtrar información confidencial.

2.3 Footprinting a través de redes sociales

Ingeniería social



La Ingeniería Social en Seguridad de la Información se refiere a la técnica de manipulación psicológica. Este truco se utiliza para recopilar información de diferentes redes sociales y otras plataformas de personas por fraude, hackeo y obtener información por estar cerca del objetivo.

Footprinting usando ingeniería social en sitios de redes sociales

- Las redes sociales son una de las mejores fuentes de información entre otras fuentes.
- Los diferentes sitios de redes sociales populares y más ampliamente utilizados han hecho que sea bastante fácil encontrar a alguien, conocerlo, incluida su información personal básica y también información confidencial.
- Las funciones avanzadas de estos sitios de redes sociales también proporcionan información actualizada.



Footprinting a través de los sitios de redes sociales

Un ejemplo de footprinting a través de los sitios de redes sociales puede ser encontrar a alguien en Facebook, Twitter, LinkedIn, Instagram y mucho más.



Twitter



Facebook



YouTube



Instagram



LinkedIn

Footprinting a través de los sitios de redes sociales

- Las redes sociales no solo son una fuente de alegría, sino que también conecta a las personas de manera personal, profesional y tradicional.
- La plataforma de redes sociales puede proporcionar información suficiente de un individuo mediante la búsqueda del objetivo.
- La búsqueda de redes sociales para personas o una organización aporta mucha información, como fotos del objetivo, información personal y datos de contacto, etc.

Ingeniería social

Qué hacen los usuarios	Información	Qué obtiene el atacante
Las personas mantienen su perfil	<ul style="list-style-type: none">• Foto del objetivo.• Números de contacto.• Correos electrónicos.• Fecha de nacimiento.• Ubicación.• Detalles del trabajo.	<ul style="list-style-type: none">• Información personal sobre un objetivo, incluida información personal, foto, etc.• Ingeniería social.
La gente actualiza su estado	<ul style="list-style-type: none">• Información personal más reciente.• Ubicación más reciente.• Información de familiares y amigos.• Actividades e intereses.• Información relacionada con la tecnología.• Información de próximos eventos.	<ul style="list-style-type: none">• Información relacionada con la plataforma y la tecnología.• Ubicación del objetivo.• Lista de empleados / amigos / familia.• Naturaleza del negocio.

Recolección de información de la red social

Bill Gates

@BillGates

Sharing things I'm learning through my foundation work and other interests.

Seattle, WA Se unió en junio de 2009

218 Siguiendo 51,2 M Seguidores

Tweets Tweets y respuestas Multimedia Me gusta

Bill Gates retuiteó

Melinda Gates @melindagates · 15 jul.

Decision-makers can take steps right now to make sure the world recovers from this pandemic stronger, more prepared & more equal than it was before. The key: Women and girls must be at the center of the response.

Read more in my piece in [@ForeignAffairs](#).

- La foto de perfil puede identificar el objetivo; El perfil puede recopilar información personal. Al utilizar esta información personal, un atacante puede crear un perfil falso con la misma información.
- Las publicaciones tienen enlaces de ubicación, imágenes y otra información de ubicación que ayuda a identificar la ubicación de destino.
- Las líneas de tiempo y las historias también pueden revelar información sensible. Al recopilar información de interés y actividades, un atacante puede unirse a varios grupos y foros para obtener más huellas. Además, habilidades, historial de empleo, empleo actual y mucho más.

Recolección de información de la red social

- Esta es la información que se puede recopilar para usar fácilmente y determinar el tipo de negocio de una organización, tecnología y plataformas utilizadas por una organización.
- En las publicaciones, las personas publican en estas plataformas, nunca piensen lo que publican.
- Su publicación puede contener suficiente información para un atacante, o una parte de la información requerida para que un atacante obtenga acceso a sus sistemas.

Noticia

Qhipertextual

≡

SEGURIDAD

Hackean cuentas de Twitter de famosos, entre ellos Elon Musk y Bill Gates, para estafar con criptomonedas

  Ebenizer Pinedo - Jul 15, 2020 - 22:59 (CET)

Estafadores hackearon las cuentas de famosos y empresas en Twitter para intentar timar a sus seguidores con criptomonedas. Su plan tuvo éxito. Entre los perfiles afectados se encuentran Elon Musk, Bill Gates, Jeff Bezos, Barack Obama, Apple y Uber.

Hackearon las cuentas de Twitter de Elon Musk, Bill Gates, Apple, Uber, Kanye Wers, Jeff Bezos, Joe Biden, Barack Obama, Michael Bloomberg, entre otros, para intentar **estafar a sus seguidores con criptomonedas**; desafortunadamente lo están logrando. En los mencionados perfiles se publicaron mensajes que incitaban a transferir una determinada cantidad en Bitcoin para recibir otra superior a cambio. La publicación, desde luego, incluía la dirección Bitcoin como destino del pago. Al momento de escribir esta publicación, los hackers **han obtenido más de 110.000** dólares, según podemos observar a través de *Blockchain*.

Estafar criptomonedas no es lo peor: el 'hackeo' a Twitter pudo desatar un colapso a nivel mundial

En el caso de Elon Musk y Bill Gates, los hackers mencionaron que al transferir 1.000 dólares te devolverían 2.000 dólares. Sin embargo, en las publicaciones de Apple, Uber y Jeff Bezos podías pagar cualquier cantidad y te "regresarían" el doble. Pese a que todos los involucrados en el hackeo reaccionaron rápidamente y eliminaron los tweets, fueron **muchas las personas que cayeron en la estafa**. La dirección de los hackers sigue aumentando sus ingresos con el paso de los minutos.



<https://hipertextual.com/2020/07/hackean-cuentas-twitter-elon-musk-y-bill-gates-estafar-con-criptomonedas>

2.4 Consultas DNS, WHOIS

Búsqueda de WHOIS

"WHOIS" ayuda a obtener información sobre el nombre de dominio, la información de propiedad.

Dirección IP, datos de Netblock, servidores de nombres de dominio y otra información.

Los Registros Regionales de Internet (RIR) mantienen la base de datos de WHOIS.

La búsqueda de WHOIS ayuda a descubrir quién está detrás del nombre de dominio de destino.

El sistema regional de registro de Internet evolucionó, y finalmente dividió el mundo en cinco RIRs:

RIRs	Acrónimo	Ubicación
Centro de información de la red Africana	AFRINIC	África.
Registro Americano de Números de Internet	ARIN	Estados Unidos, Canadá, varias partes de la región del Caribe y la Antártida.
Centro de información de la red Asia-Pacífico	APNIC	Asia, Australia, Nueva Zelanda, y países vecinos.
Centro de información de la red de América Latina y el Caribe	LACNIC	América Latina y partes de la región del Caribe.
Centro de coordinación de la red IP Européens de Réseaux	RIPE NCC	Europa, Rusia, Medio Oriente y Asia Central.

Ejecutando Footprinting de WHOIS

1. Vaya a la URL <https://www.whois.com/>



Análisis de resultados de búsqueda de WHOIS

2. Una búsqueda del dominio de destino.



The screenshot shows the Whois.com homepage with the logo 'Whois Identity for everyone'. Below the logo is a navigation bar with links: DOMAINS, WEBSITE, CLOUD, HOSTING, and SERVERS. The main search field contains the domain 'ipspecialist.net'. Under the search field, there is a section titled 'Domain Information' with the following details:

Domain:	ipspecialist.net
Registrar:	Amazon Registrar, Inc.
Registered On:	2016-08-24
Expires On:	2023-08-24
Updated On:	2020-03-27
Status:	clientTransferProhibited
Name Servers:	ns-1260.awsdns-29.org ns-127.awsdns-15.com ns-1666.awsdns-16.co.uk ns-834.awsdns-40.net

To the right of the search results, there is a large box titled 'Raw Whois Data' containing the following text:

```
Domain Name: ipspecialist.net
Registry Domain ID: 2054790973_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.registrar.amazon.com
Registrar URL: https://registrar.amazon.com
Updated Date: 2020-03-27T07:57:15.645Z
Creation Date: 2016-08-24T12:40:08Z
Registrar Registration Expiration Date: 2023-08-24T12:40:08Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: registrar-abuse@amazon.com
Registrar Abuse Contact Phone: +1.2067406200
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: renewPeriod https://icann.org/epp#renewPeriod
Registry Registrant ID:
Registrant Name: On behalf of ipspecialist.net owner
Registrant Organization: Whois Privacy Service
Registrant Street: P.O. Box 81226
Registrant City: Seattle
Registrant State/Province: WA
Registrant Postal Code: 98108-1226
Registrant Country: US
Registrant Phone: +1.2065771368
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: owner-3779216@ipspecialist.net.whoisprivacyservice.org
Registry Admin ID:
Admin Name: On behalf of ipspecialist.net administrative contact
Admin Organization: Whois Privacy Service
Admin Street: P.O. Box 81226
Admin City: Seattle
Admin State/Province: WA
Admin Postal Code: 98108-1226
Admin Country: US
Admin Phone: +1.2065771368
```

Resultados de la búsqueda

Muestra el perfil de dominio completo, que incluye:

- Información del registrante
- País del registrante
- Dirección IP
- ASN
- Historial de WHOIS
- Historia del registrador
- Organización registrada
- Información del servidor de nombres de dominio
- Ubicación de IP
- Estado del dominio
- Historial de IP,
- Historial de alojamiento

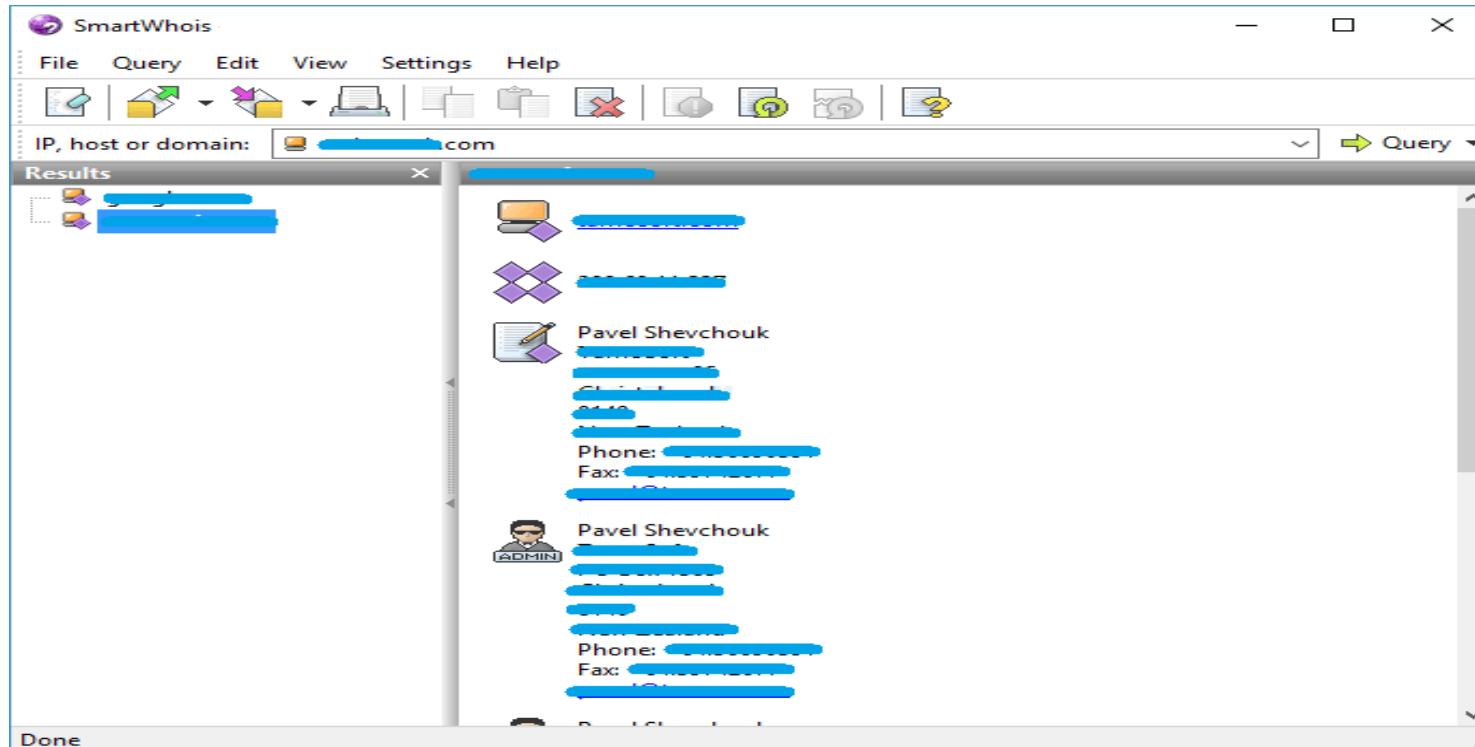
También incluye otra información, como correo electrónico y dirección postal del registrador y administrador, junto con los datos de contacto.

- ❑ Puede ir a <https://whois.domaintools.com> para ingresar la URL de destino para la información de búsqueda whois.



Aplicación de búsqueda SmartWhois

- Puede descargar el software "SmartWhois" de www.tamos.com para la búsqueda de Whois como se muestra en la figura a continuación:



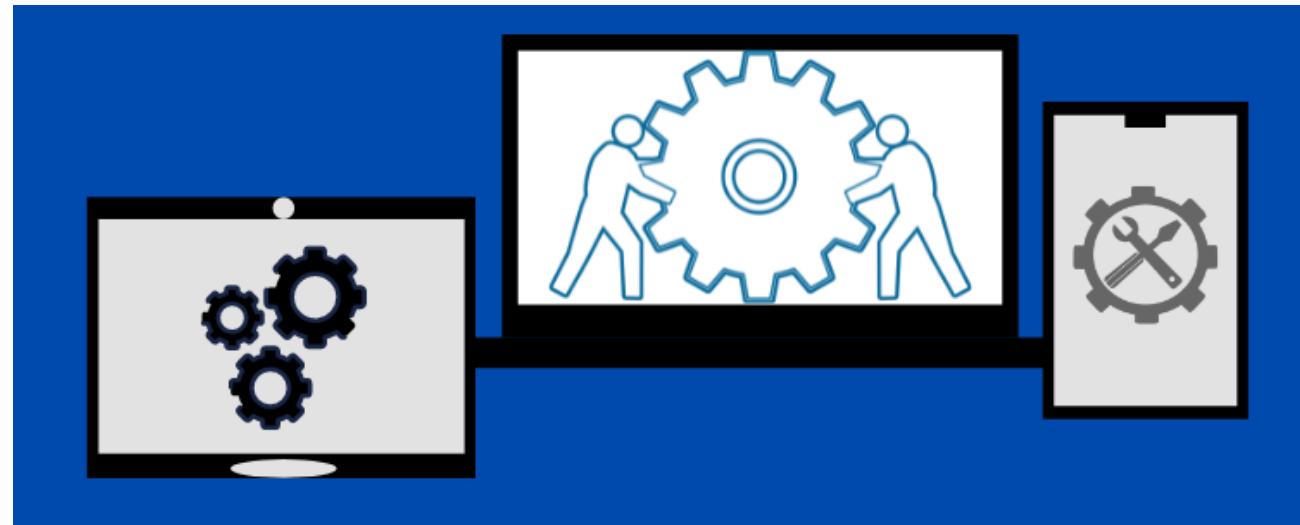
Herramientas de búsqueda de WHOIS

Las herramientas que funcionan con diferentes desarrolladores en la búsqueda de WHOIS se enumeran a continuación:

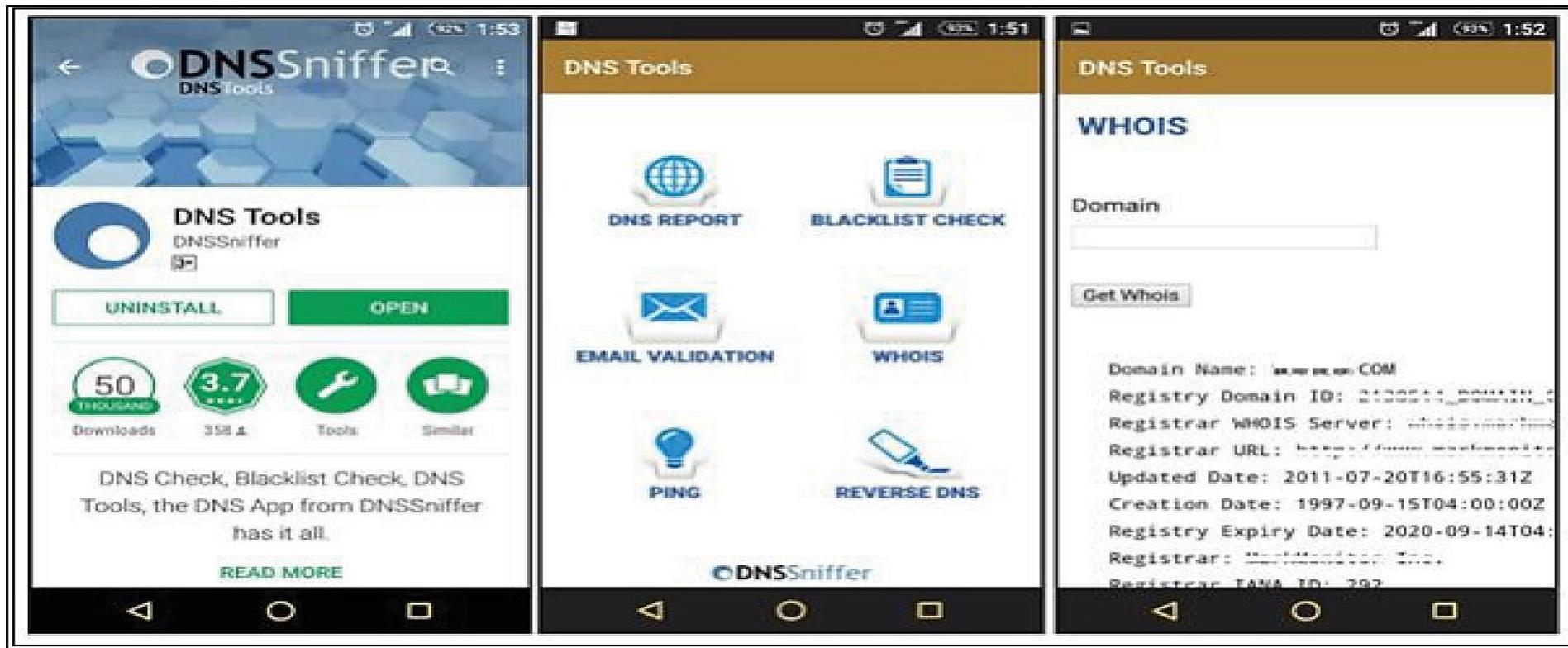
- ❑ <http://lantricks.com>
- ❑ <http://www.networkmost.com>
- ❑ <http://tialsoft.com>
- ❑ <http://www.johnru.com>
- ❑ <https://www.calleripro.com>
- ❑ <http://www.nirsoft.net>
- ❑ <http://www.sobelsoft.com>
- ❑ <http://www.softfuse.com>

Herramientas de búsqueda de WHOIS para dispositivos móviles

- ❑ La aplicación "DNS Tools" de www.dnssniffers.com está disponible en Google Play Store.
- ❑ Incluye otras características, como Informe de DNS, Verificación de lista negra, Validación de correo electrónico, WHOIS, ping y reversa DNS.



Aplicación "DNS Tools"

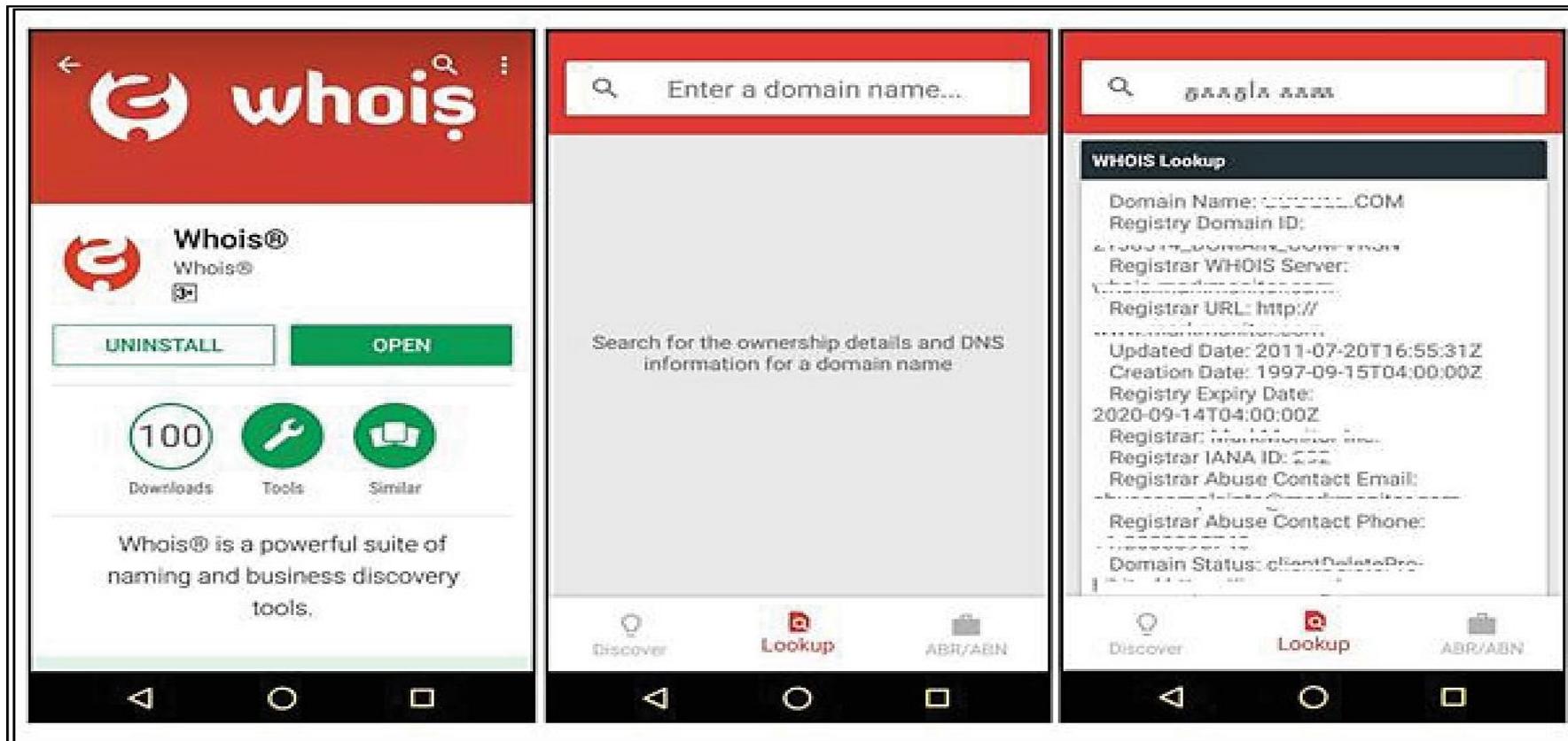


Aplicación whois® de www.whois.com.au

Aplicación whois® de www.whois.com.au en Google Play Store para mirar.

- Búsqueda de WHOIS
- Búsqueda de DNS
- Búsqueda RBL
- Traceroute
- Búsqueda de IP
- Acceso a datos a granel / API

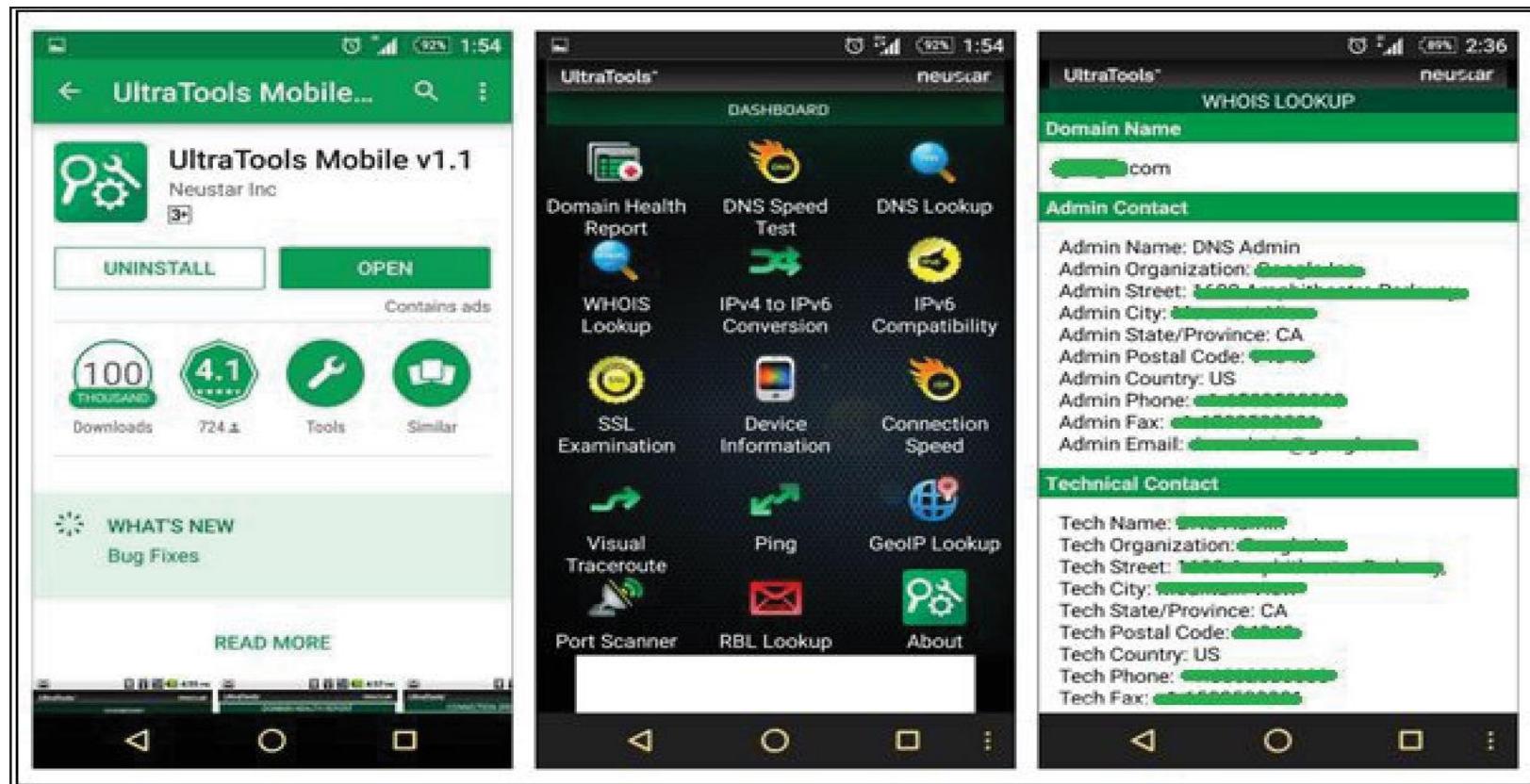
Aplicación WHOIS



www.ultratools.com ofrece ultra Tools Mobile

Esta aplicación ofrece múltiples funciones como informe de estado del dominio, prueba de velocidad de DNS, búsqueda de DNS, búsqueda de Whois, ping y otras opciones.

Aplicación Ultra Tools Mobile



Footprinting DNS

- La información de búsqueda de DNS es útil para identificar un host dentro de una red de destino.
- Hay varias herramientas disponibles en Internet que realizan búsquedas de DNS.
- Antes de continuar con las herramientas de búsqueda de DNS y el resumen de resultados de estas herramientas de DNS, debe conocer los símbolos de tipo de registro DNS y significa:



Tipos de Registro DNS

Tipo de Registro	Descripción
A	La dirección IP del host.
MX	Servidor de correo del dominio.
NS	Servidor de nombres de host.
CNAME	La denominación canónica permite alias a un host.
SDA	Indicar autoridad para el dominio.
SRV	Registros de servicio.
PTR	Mapeo de host IP.
RP	Persona responsable.
HINFO	Información del anfitrión.
TXT	Registros no estructurados.

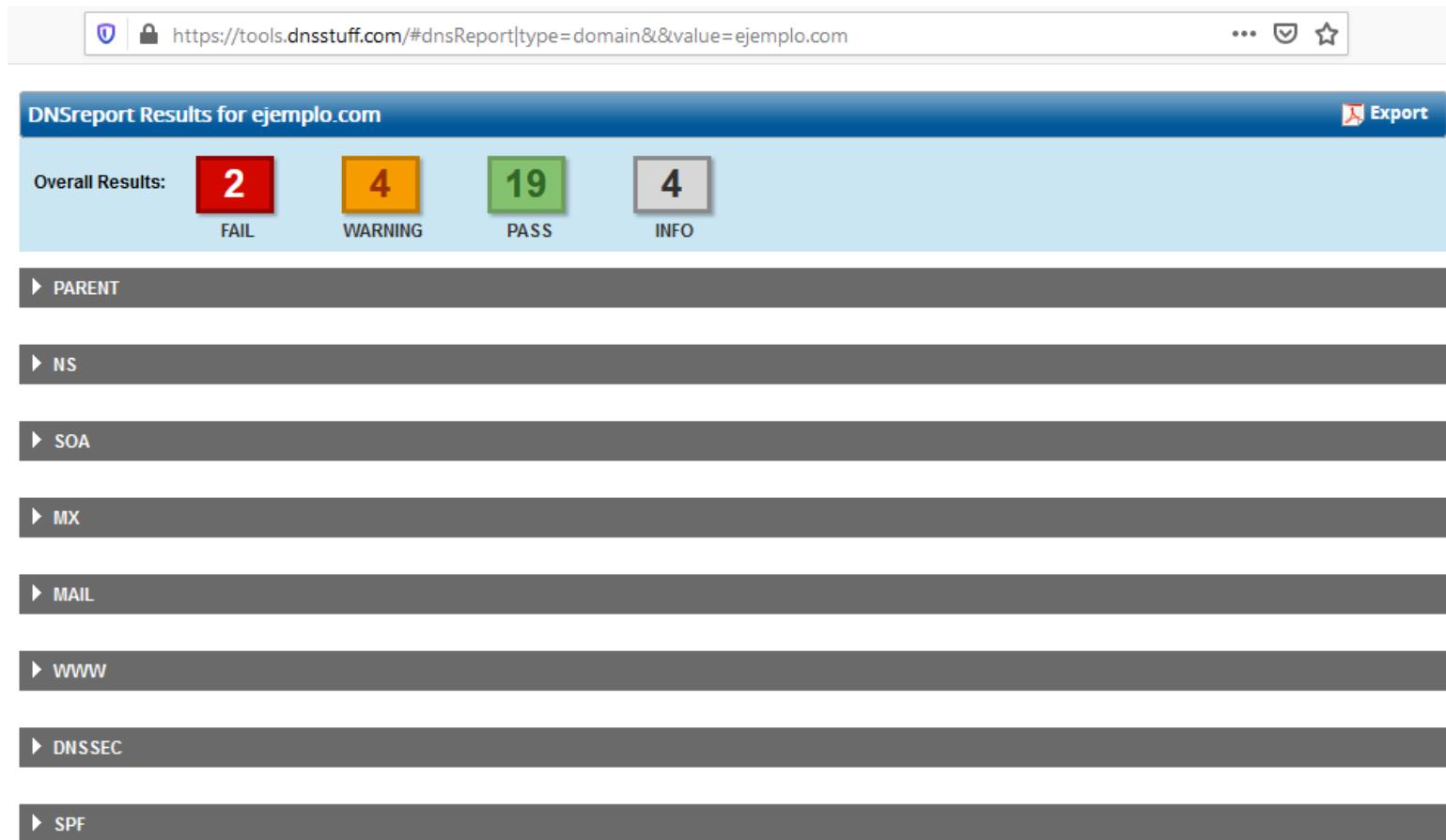
Extracción de información de DNS utilizando DNSStuff

Ir a la URL: <https://www.dnsstuff.com>

The screenshot shows the homepage of the DNSStuff website at https://tools.dnsstuff.com. The interface is organized into several sections:

- Header:** Shows the URL in the address bar and navigation icons.
- Tool Categories:** A horizontal menu with tabs: All Tools, Domain/WWW Tools (highlighted), IP Tools, Networking Tools, Email Tools, and Free Tools & Trials.
- Domain Tools:** A main section containing several sub-tools:
 - DNSreport:** A tool to check for DNS problems. It has a search bar with "ejemplo.com" and a blue "▶" button. This tool is highlighted with a red box.
 - WHOIS/IPWHOIS Lookup:** A tool to get contact info for a domain/IP. It has a search bar with "www.domain.com [or] 11.11.11.11" and a blue "▶" button.
 - WWW Co-host Tool:** A tool to find websites hosted on a specific IP. It has a search bar with "domain.com [or] 11.11.11.11" and a blue "▶" button.
 - Top Level Domain (TLD) Lookup:** A tool to find available domains. It has a search bar with "domain.com" and a blue "▶" button.
 - Abuse Lookup:** A tool to find abuse contact for a domain. It has a search bar with "domain.com" and a blue "▶" button.
 - ISP Cached DNS Lookup:** A tool to find DNS servers with cached entries. It has a search bar with "domain.com [or] 11.11.11.11" and a dropdown menu for "Choose a DNS record type".
 - Website Info:** A tool to gather technical information from a website. It has a "RUN TEST ▶" button.
 - DNS Lookup:** A tool to look up DNS records. It has a search bar with "[www] domain.com [or] 11.11.11.11", a dropdown menu for "Choose a DNS record type", an "Optional Server" field, and a "Select additional display type" dropdown.

Extracción de información de DNS utilizando DNSStuff



La figura muestra la salida de “ejemplo.com”.

Extracción de información de DNS utilizando DNSStuff

DNSreport Results for ejemplo.com			
Overall Results:			
Status	Test Name	Information	
FAIL	2	WARNING	4
PASS	Parent zone provides NS records	Parent zone exists and provides NS records. This is good because some domains, usually third or fourth level domains, such as 'example.co.us' do not have a direct parent zone. This is legal but can cause confusion. The NS Records provided are (nameserver IP Address TTL): ns1.sedoparking.com. 91.195.241.8 ns2.sedoparking.com. 91.195.240.8	4
PASS	Number of nameservers	At least 2 (RFC2182 section 5 recommends at least 3), but fewer than 8 NS records exist (RFC1912 section 2.8 recommends that you have no more than 7). This meets the RFC minimum requirements, but is lower than the upper limits that some domain registrars have on the number of nameservers. A larger number of nameservers reduce the load on each and, since they should be located in different locations, prevent a single point of failure. The NS Records provided are: ns1.sedoparking.com. 91.195.241.8 TTL=172800 ns2.sedoparking.com. 91.195.240.8 TTL=172800	
▼ NS			
Status	Test Name	Information	
PASS	Unique nameserver IPs	All nameserver addresses are unique. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data: ns1.sedoparking.com. 91.195.241.8 ns2.sedoparking.com. 91.195.240.8	
PASS	All nameservers respond	All nameservers responded. We were able to get a timely response for NS records from your nameservers, which indicates that they are running correctly and your zone (domain) is valid. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data:	

Como se muestra en el siguiente resultado, puede expandir los campos deseados para obtener información detallada.

Extracción de información de DNS utilizando el Dossier de dominio

Vaya al sitio web <https://centralops.net/co> e ingrese la dirección IP del dominio que desea buscar.

The screenshot shows the Central Ops .net website interface. The top navigation bar includes the logo 'Central Ops .net' and the tagline 'Advanced online Internet utilities'. On the left, a sidebar titled 'Utilities' lists various tools: Domain Dossier, Domain Check, Email Dossier, Brower Mirror, Ping, Traceroute, NsLookup, AutoWhois, and AnalyzePath. The main content area is titled 'Domain Dossier' with the subtitle 'Investigate domains and IP addresses'. It features a search field labeled 'domain or IP address' containing a redacted URL. Below the search field are several checkboxes: 'domain whois record' (checked), 'network whois record' (checked), 'DNS records' (unchecked), 'traceroute' (unchecked), and 'service scan' (unchecked). A 'go' button is located next to the service scan checkbox. At the bottom, it shows the user is anonymous, has a balance of 48 units, and provides links for 'log in' and 'account info'. The 'Central Ops .net' logo is also present at the bottom right.

Extracción de información de DNS utilizando el Dossier de dominio

El resultado trae el nombre canónico, alias, dirección IP, registros whois de dominio, registros whois de red y registros DNS.

The screenshot shows a web interface for CentralOps.net, a service provided by Hexillion. The main content area displays a table titled "DNS records". The table has columns for "name", "class", "type", "data", and "time to live". The data in the table is as follows:

name	class	type	data	time to live
[REDACTED].com	IN	A	[REDACTED]	300s (00:05:00)
[REDACTED].com	IN	AAAA	[REDACTED]	300s (00:05:00)
[REDACTED].com	IN	NS	[REDACTED]	345600s (4.00:00:00)
[REDACTED].com	IN	NS	[REDACTED]	345600s (4.00:00:00)
[REDACTED].com	IN	NS	[REDACTED]	345600s (4.00:00:00)
[REDACTED].com	IN	MX	preference: 30 exchange: [REDACTED]	600s (00:10:00)
[REDACTED].com	IN	TXT	[REDACTED] verification=[REDACTED]	3600s (01:00:00)
[REDACTED].com	IN	TXT	docusign=[REDACTED]	300s (00:05:00)
[REDACTED].com	IN	CAA	[no interpretation available] hex dump: (15 bytes) 00 05 69 73 73 75 65 70 ..issuem 6B 69 2E 67 6F 6F 67 [REDACTED]	86400s (1.00:00:00)
[REDACTED].com	IN	TXT	[REDACTED]	3600s (01:00:00)
[REDACTED].com	IN	MX	preference: 50 exchange: [REDACTED]	600s (00:10:00)

Herramientas de interrogación de DNS

❑ Hay muchas herramientas en línea disponibles para la información de búsqueda de DNS, algunas de ellas se enumeran a continuación:

- <http://www.dnsstuff.com>
- <http://www.kloth.net>
- <http://www.nirsoft.net>
- <http://www.domaintools.com>
- <http://www.ultratools.com>
- <http://www.webmaster-toolkit.com>
- <http://network-tools.com>
- <http://www.mydnstools.info>
- <http://www.dnswatch.info>
- <http://www.dnsqueries.com>

2.5 Google hacking

Operadores de búsqueda avanzada de Google

Algunas opciones avanzadas se pueden utilizar para buscar un tema específico mediante motores de búsqueda. Estos operadores de búsqueda avanzada hicieron que la búsqueda fuera más apropiada y se centrara en un tema determinado.



Operadores de búsqueda avanzada de Google

Operadores de búsqueda avanzada	Descripción
site	Busca el resultado en el dominio dado.
related	Busca páginas web similares.
cache	Muestra las páginas web almacenadas en la caché.
link	Enumera los sitios web que tienen un enlace a una página web específica.
allintext	Busca sitios web que contengan una palabra clave específica.
intext	Busca documentos que contengan una palabra clave específica.
allintitle	Busca sitios web que contengan una palabra clave específica en el título.
intitle	Busca documentos que contengan una palabra clave específica en el título.
allinurl	Busca sitios web que contengan una palabra clave específica en URL.
inurl	Busca documentos que contengan una palabra clave específica en URL.

Para la Búsqueda avanzada de Google, también puede ir a la siguiente URL:

Búsqueda avanzada de Google X +

https://www.google.com/advanced_search

Búsqueda avanzada

Mostrar páginas que contengan...

todas estas palabras:

esta palabra o frase exactas:

cualquiera de estas palabras:

ninguna de estas palabras:

números del: al

Para hacer esto en el cuadro de búsqueda

Ingresá las palabras importantes: Terrier ratonero tricolor.

Ingresá las palabras exactas entre comillas: "Terrier ratonero".

Ingresá OR entre las palabras que deseas: En miniatura OR estándar.

Ingresá un signo menos justo delante de las palabras que no deseas que aparezcan: -Roedor, -"Jack Russell".

Ingresá dos puntos entre los números y agrega una unidad de medida: 10..25 lb, \$300..\$500, 2010..2011.

Luego restringe tus resultados por...

idioma: cualquier idioma

región: cualquier región

última actualización: en cualquier momento

sitio o dominio:

términos que aparecen: En cualquier parte de la página

SafeSearch Mostrar los resultados más relevantes

tipo de archivo: Cualquier formato

derechos de uso: Páginas cuyo uso no requiera de licencias

Busca páginas en el idioma que seleccionas.

Busca páginas publicadas en una región determinada.

Busca páginas actualizadas en el transcurso del período que específicas.

Realiza búsquedas en un sitio (como wikipedia.org) o restringe los resultados a un dominio como .edu, .org o .gov.

Busca términos en toda la página, en su título o en su dirección web, o vínculos que te dirijan a la página que estás buscando.

Indica a SafeSearch si quieres que filtre contenido sexualmente explícito.

Busca páginas del formato que prefieras.

Busca páginas que puedas usar libremente.

Búsqueda avanzada

https://www.google.com/advanced_search

Base de datos de hackeo de Google (GHDB)

Hackeo de Google, Google Dorking es una combinación de técnicas de hackeo de computadoras que encuentran los problemas de seguridad dentro de la red y los sistemas de una organización utilizando la búsqueda de Google y otras aplicaciones con tecnología de Google.



Base de datos de hackeo de Google (GHDB)

Google Hacking popularizado por Johnny Long. Clasificó las consultas en una base de datos conocida como Google Hacking Database (GHDB). Esta base de datos categorizada de consultas está diseñada para descubrir la información. Esta información puede ser confidencial y no estar disponible públicamente. El hackeo de Google se utiliza para acelerar las búsquedas.



Base de datos de hackeo de Google

Como se muestra en la figura, a través de www.exploit-db.com, puede buscar en GHDB o explorar la categoría de GHDB. Del mismo modo, www.hackersforcharity.org es también una plataforma en línea para GHDB.

Ingresé la siguiente URL: <https://www.exploit-db.com/google-hacking-database/>

Base de datos de hackeo de Google

The screenshot shows a web browser window titled "Google Hacking Database (GHD)" with the URL <https://www.exploit-db.com/google-hacking-database>. The page has a dark blue header with the "EXPLOIT DATABASE" logo and navigation icons. On the left, there's a vertical orange sidebar with various icons. The main content area is titled "Google Hacking Database". It features a search bar with "Quick Search" and filters, and a table listing items from July 2020. The columns are "Date Added", "Dork", "Category", and "Author".

Date Added	Dork	Category	Author
2020-07-17	inurl:wp-content/plugins/lifterlms	Advisories and Vulnerabilities	Sachin Kattimani
2020-07-17	intitle:"Wing FTP Server - Web"	Vulnerable Servers	Alexandros Pappas
2020-07-17	inurl:wp-content/plugins/all-in-one-wp-migration	Advisories and Vulnerabilities	Sachin Kattimani
2020-07-17	inurl:wp-content/plugins/async-javascript	Advisories and Vulnerabilities	Sachin Kattimani
2020-07-17	inurl:wp-content/plugins/idx-broker-platinum	Advisories and Vulnerabilities	Sachin Kattimani
2020-07-17	inurl:wp-content/plugins/wpjobboard	Advisories and Vulnerabilities	Sachin Kattimani
2020-07-16	inurl:wp-content/plugins/wd-google-maps	Advisories and Vulnerabilities	Sachin Kattimani
2020-07-16	inurl:wp-content/plugins/sendpress	Advisories and Vulnerabilities	Abhi Chitkara
2020-07-16	allintext:username,password filetype:log	Files Containing Juicy Info	isa gojaria
2020-07-14	inurl:wp-content/plugins/kingcomposer	Advisories and Vulnerabilities	Abhi Chitkara

Hacking de Google

La base de datos de hacking de Google proporciona la información actualizada que es útil para la explotación, como puntos de apoyo, directorios sensibles, archivos vulnerables, mensajes de error y mucho más.



¡Muchas gracias!



PCM | Secretaría de Gobierno
y Transformación Digital

CENTRO NACIONAL DE SEGURIDAD DIGITAL

