Algunas herramientas para el *footpringting*

Readnotify.com

Se puede utilizar esta herramienta de recopilación y creación de enlaces para ahorrar tiempo y saber cuándo seguir con más correos electrónicos, en caso de que el destinatario haya abierto el correo electrónico, pero nunca haya respondido, podrían haber olvidado responder, o algo podría haber perturbado su atención. Este tipo de herramientas se utilizan para:

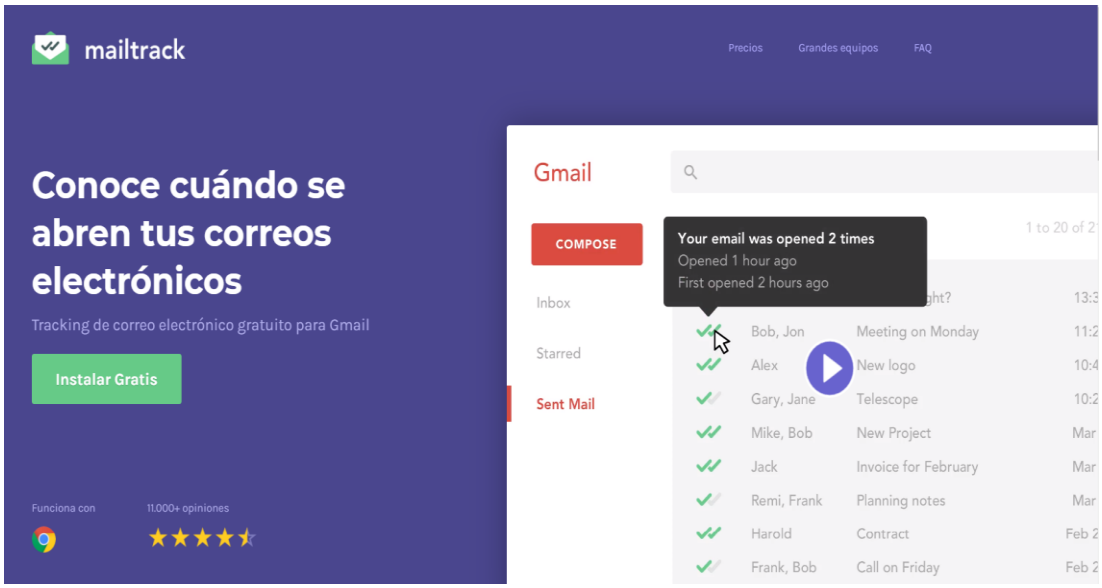
- ✓ Cuando se recibió el correo electrónico y la lectura.
- ✓ Enviar mensajes de correo electrónico destructivos.
- ✓ Localización GPS y el mapa del destinatario.
- ✓ El tiempo dedicado a la lectura de los mensajes de correo electrónico.
- ✓ Sea o no el destinatario visitó los enlaces que se les envió.
- ✓ Seguimiento de PDF y otros tipos de archivos adjuntos.
- ✓ Establecer mensajes de expiración después de un tiempo especificado.

http://www.readnotify.com/

ReadNotify es un servicio de rastreo original en su clase, y es uno de los servicios de correo electrónico y de rastreo de documentos más usados en el mundo hoy en día. ReadNotify le dice cuando sus correos electrónicos y documentos rastreados son abiertos / reabiertos / reenviados y mucho más.

Mailtrack

Es una herramienta de seguimiento de correo electrónico que informa si sus correos electrónicos han sido abiertos o no, y cuántas veces, a través de su sistema de seguimiento basado en píxeles, también le permite saber cuándo los correos electrónicos que recibe están siendo rastreados, con el indicador de correo electrónico rastreado entrante de *Mailtrack*.



https://mailtrack.io/es/

Otro tipo de herramientas que sirven para rastrear correos electrónicos se encuentran en las siguientes direcciones:

Herramienta	URL
MailTracker	https://hunter.io/mailtracker
Lead Boxer	https://www.leadboxer.com
Boomerang	https://www.boomeranggmail.com

¿Cómo funciona el rastreo de correo electrónico abierto?

En el caso de **Mailtracker**, se utiliza el seguimiento basado en píxeles, cuando se envía un correo electrónico, Mailtracker añade automáticamente un píxel de seguimiento (una imagen muy pequeña) a ese correo electrónico. Luego, cuando se abre, el píxel de seguimiento se descarga y envía una llamada a nuestros servidores para informarnos que el correo se ha abierto.

Google Workspace ofrece una opción de acuse de recibo de lectura, pero está limitada a los clientes de Google; su concepto y tecnología son extremadamente limitados. Así es como Outlook realiza el seguimiento de la apertura del correo, pero es mucho menos fiable que el seguimiento basado en píxeles. Los recibos de lectura dependen de que el destinatario acepte el acuse de recibo del correo electrónico, lo cual no siempre está garantizado.

El seguimiento de los correos electrónicos que se abren con Google Analytics también funciona utilizando píxeles de seguimiento, pero el proceso de seguimiento es mucho más complicado y lleva mucho más tiempo.

Google Hacking

Los términos *hacking*, *hacks* o *dorking* de Google se refieren a los ataques que utilizan Google u otros motores de búsqueda para encontrar servidores y sitios web vulnerables. Google

hacking se basa en la invención de consultas de búsqueda específicas, a menudo utilizando comodines y operadores de búsqueda avanzada (como *intitle, inurl, intext, filetype*, y más), para localizar servidores web y páginas web mal configurados que exponen información sensible, por ejemplo, una búsqueda de *site*: */signup/password.php podría revelar todas las páginas que contienen portales de acceso.

La Base de Datos de Hacking de Google (GHDB) es un compendio de términos de búsqueda de hacking de Google que se ha descubierto que revelan datos sensibles expuestos por servidores y aplicaciones web vulnerables, La GHDB fue lanzada en el 2000 por Johnny Long para servir a los probadores de penetración. En 2010, Long entregó la base de datos a Offensive Security y se convirtió en parte de exploit-db.com. También se amplió para incluir no sólo el motor de búsqueda de Google, sino también otros motores de búsqueda como el Bing de Microsoft, así como otros repositorios como GitHub.

Operadores más populares de Google Dork

El motor de búsqueda de Google tiene su propio lenguaje de consulta incorporado, la siguiente lista de consultas puede ser ejecutada para encontrar una lista de archivos, encontrar información sobre su competencia, rastrear personas, obtener información sobre vínculos de retroceso SEO, construir listas de correo electrónico y, por supuesto, descubrir vulnerabilidades de la web.

- ✓ **cache:** este mostrará la versión en caché de cualquier sitio web.
- ✓ **allintext:** busca un texto específico contenido en cualquier página web.
- ✓ **allintitle:** igual que allintext, pero mostrará páginas que contengan títulos con caracteres.
- ✓ **allinurl:** puede utilizarse para obtener resultados cuya URL contenga todos los caracteres especificados.
- ✓ **Type:** se utiliza para buscar cualquier tipo de extensión de archivo, por ejemplo, si se desea buscar archivos jpg se puede utilizar: type: jpg.
- ✓ **inurl:** es exactamente lo mismo que allinurl, pero sólo es útil para una única palabra clave, por ejemplo, inurl: admin.
- ✓ **intitle:** se utiliza para buscar varias palabras clave dentro del título.
- ✓ **inanchor:** es útil cuando se necesita buscar un texto de anclaje exacto utilizado en cualquier enlace.
- ✓ **intext:** útil para localizar páginas que contienen ciertos caracteres o cadenas dentro de su texto.
- ✓ **link:** mostrará la lista de páginas web que tienen enlaces al URL especificado.
- ✓ **site:** le mostrará la lista completa de todos los URL indexados para el dominio y subdominio especificado.

Las personas, a menudo, toman a Google como un simple motor de búsqueda usado para encontrar texto, imágenes, videos y noticias. Sin embargo, en el mundo de la información, tiene un papel muy amplio. Google también puede ser usado como una herramienta de *hacking* muy útil.

No se pueden piratear sitios web directamente con Google, pero sus enormes capacidades de rastreo web pueden ser de gran ayuda para indexar casi cualquier cosa dentro de cualquier sitio web que incluya información sensible, esto puede incluir desde el nombre de usuario, la contraseña y otras vulnerabilidades generales que ni siquiera conocerá, básicamente, con Google Dorking puedes encontrar las vulnerabilidades de cualquier aplicación y servidor web con la ayuda del motor de búsqueda nativo de Google.

- ✓ **SearchDiggity 3.1:** herramienta que permite realizar Google Hacking y búsquedas avanzadas en otros sitios como Bing y SHODAN a través de Proxies. https://resources.bishopfox.com/resources/tools/Google hacking diggity/attack tools/

- ✓ **Google Hack 1.6:** es una herramienta que permite realizar búsquedas avanzadas en Google mediante una interfaz gráfica, simplemente seleccionas el tipo de búsqueda que esperas obtener. https://sourceforge.net/projects/googlehacks/files/Googlehacks/Google%20Hacks%201.6/

- ✓ **PaGoDo:** (Passive Google Dork) es una herramienta de OSINT que te permite automatizar el hacking de Google. https://github.com/opsdisk/pagodo

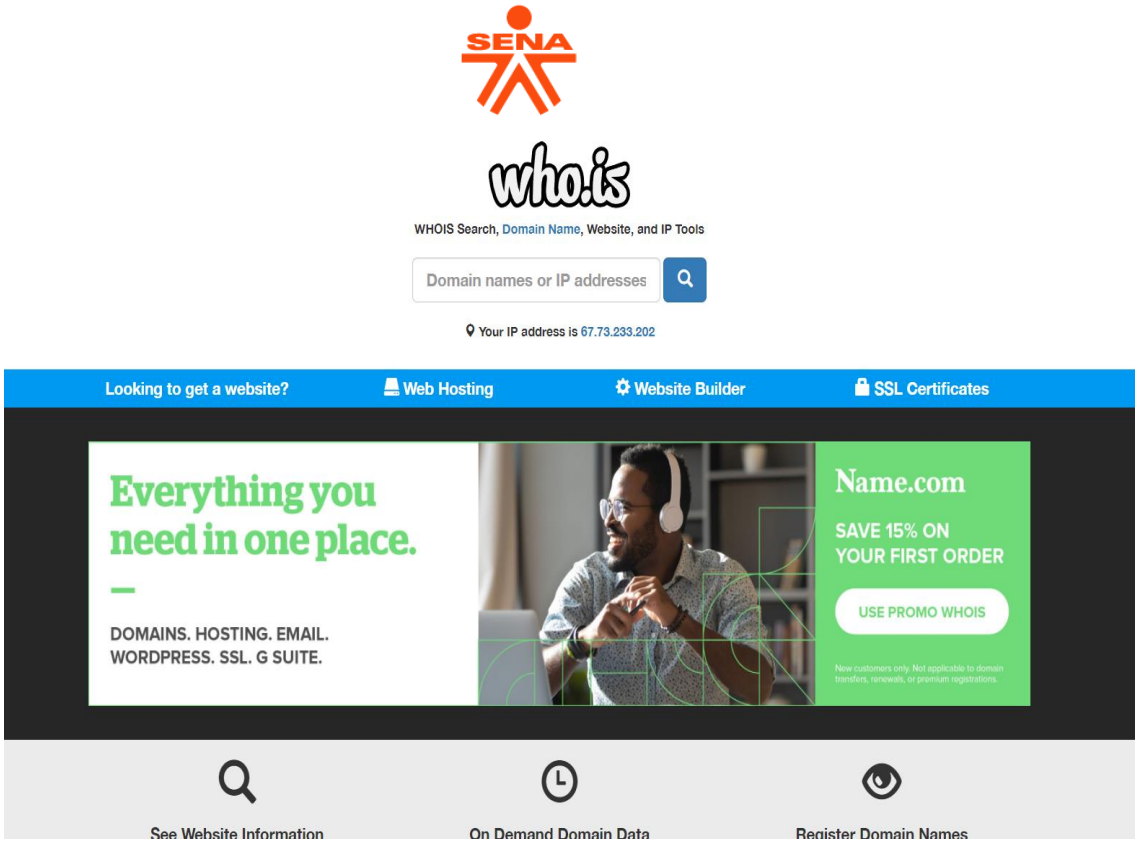
Google casi siempre indexa todo lo relacionado con Internet, que también incluye diferentes informaciones privadas de servicios mal configurados, esto puede ser a veces útil e incluso igualmente dañino al mismo tiempo, es necesario que se asegure de que no acceda a ninguno de los servicios, incluso si la contraseña está expuesta, ya que esto podría meterle en problemas por no tener autorización; sin embargo, si tiene algún servicio alojado en línea, puede utilizar algunos de los comandos de dork en su dominio para asegurarse de que no dejó nada expuesto que el delincuente pueda utilizar para afectarle.

Herramientas de *footprinting*

- ✓ **WHOIS:** WHOIS es un directorio público mediante el cual puede saber «quién es» («who is» en inglés) el propietario de un dominio o dirección IP, antes podía utilizar WHOIS para conocer algunos datos del propietario, como su nombre, dirección, número de teléfono y dirección de correo electrónico.

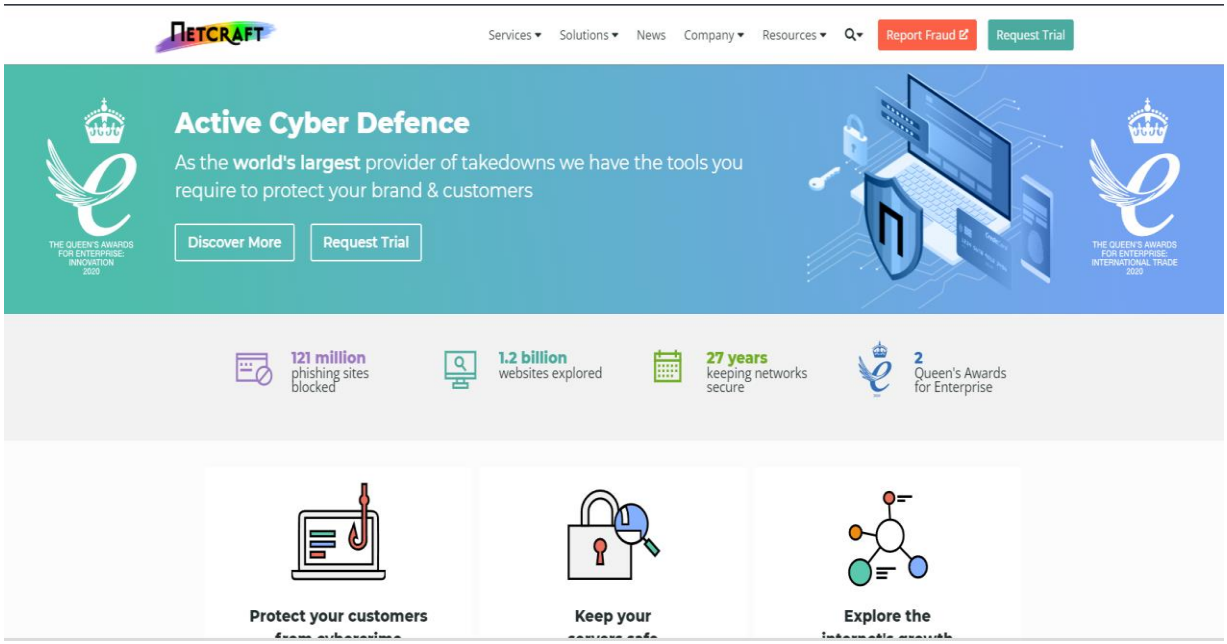
  No obstante, dado que el RGPD entró en vigor en mayo de 2018, casi toda la información de los propietarios de dominio ahora aparece oculta, se trata de una medida provisoria mientras la ICANN determina cómo utilizar la base de datos de WHOIS sin incumplir el RGPD, eso significa que la ICANN puede hacer que (parte) de esa información vuelva a ser pública en el futuro.

  Aunque para la mayoría de los dominios, los detalles sobre el propietario están ocultos, puedes encontrar información útil en el directorio WHOIS, puedes ver cuándo expirará el dominio, cuál es el estado de la transferencia, quién es el encargado del registro del dominio, a quién contactar en caso de abuso y qué servidores de nombres se están utilizando, si quiere obtener información sobre un dominio en particular, utiliza la página de búsqueda en WHOIS, allí también podrás completar un formulario para ponerse en contacto con el propietario de cualquier dominio alojado en one.com. obviamente, es decisión del propietario contestarle o no.



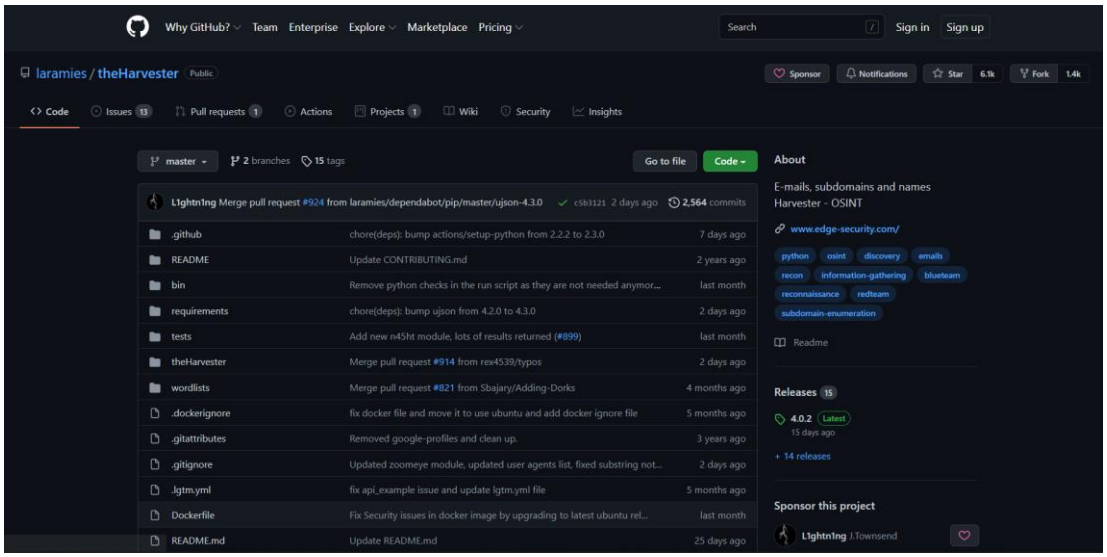
http://who.is

✓ **Netcraft:** es una empresa de servicios de internet con sede en el Reino Unido que presta servicios de seguridad en internet, entre ellos, la desarticulación de delitos cibernéticos, el análisis de la seguridad de las aplicaciones y la exploración automatizada de vulnerabilidades, le permite conocer la infraestructura y las tecnologías utilizadas por cualquier sitio utilizando los resultados de la minería de datos de Internet propia de Netcraft.



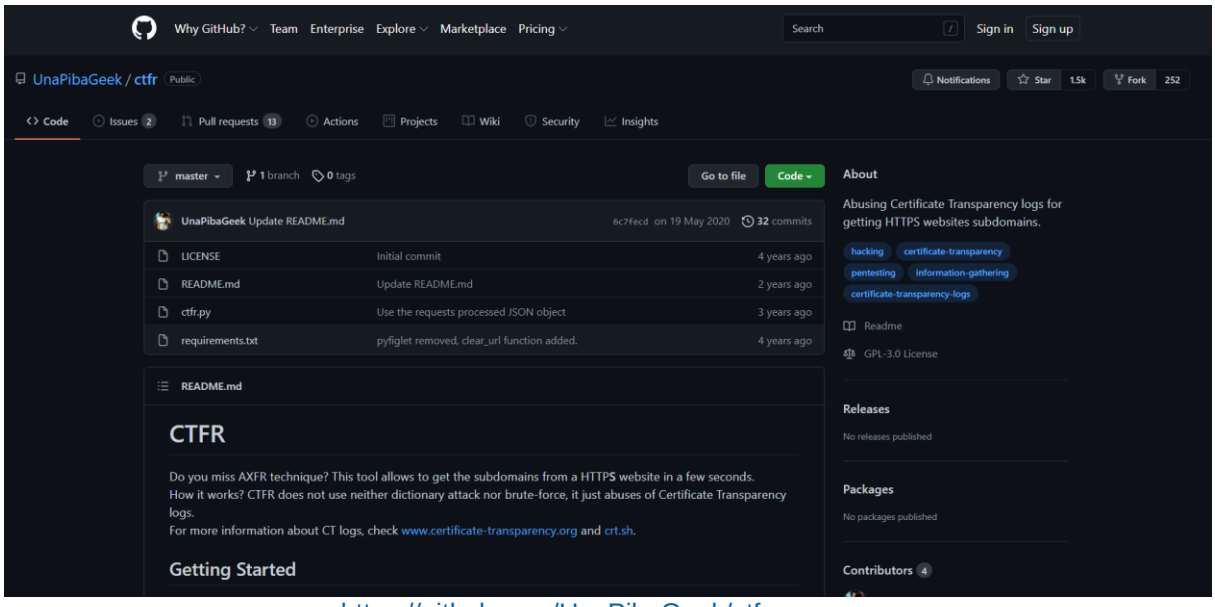
https://www.netcraft.com

✓ **TheHarvester:** es una herramienta muy sencilla de usar, pero poderosa y eficaz, diseñada para ser utilizada en las primeras etapas de una prueba de penetración, se usa para la recopilación de inteligencia de código abierto (OSINT) para ayudar a determinar el panorama de amenazas externas de una empresa en Internet. La herramienta reúne correos electrónicos, nombres, subdominios, IP y URL usando múltiples fuentes de datos públicos**.**



https://github.com/laramies/theHarvester

✓ **CTFR:** es una herramienta creada por Sheila A. Berta que abusa de los logs de los certificados SSL mediante la transparencia de certificados gracias al buscador de certificados crt.sh, con esta herramienta se pueden enumerar automáticamente subdominios ocultos que pueden contener información sensible o ser zonas explotables gracias consultas a crt.sh.



https://github.com/UnaPibaGeek/ctfr

CTFR no usa ataque de diccionario ni fuerza bruta, solo abusa de los registros de transparencia de certificado, el proyecto de transparencia de certificados (CT) representa una estructura abierta para el monitoreo y auditoría de la emisión de certificados SSL por Autoridades Certificadoras (AC), que permite detectar el mal uso de certificados o emisiones hechas de manera inadecuada, la transparencia es lograda ya que las Autoridades Certificadoras tienen que colocar/ingresar los certificados en registros accesibles y calificados de CT, permitiendo que los clientes puedan monitorear los registros para visualizar los certificados emitidos para sus dominios y así posibilitar la detección de posibles fraudes en pocos minutos**.**

Herramientas adicionales de interés

- ✓ https://github.com/rbsec/dnscan
- ✓ http://www.dnsdigger.com
- ✓ http://ghh.sourceforge.net
- ✓ http://code.Google.com