Hoja de trucos de OSINT

Hackeo de Google

Google dorking, también conocido como **Google hacking,** puede devolver información que es difícil de localizar a través de consultas de búsqueda simples. Con esta técnica, se puede descubrir información que no está destinada al acceso público.

Google **Hacking Database** (GHDB) es una fuente autorizada para consultar el alcance cada vez mayor del motor de búsqueda de Google.
Su contenido son términos de búsqueda, que permiten encontrar nombres de usuario, contraseñas e incluso archivos que contienen información sensible. El GHDB se encuentra aquí: https://www.exploit-db.com/google-hacking-database/

Operadores de búsqueda de Google y Bing

Operador	Descripción
"Término de búsqueda"	Busque la frase exacta dentro de **" "**
-	Eliminar las páginas que mencionan un término determinado de los resultados de búsqueda
+	Obligar a Google a devolver palabras comunes que normalmente se descartarían
O	Buscar un término de búsqueda dado U otro término
sitio:	Buscar dentro de un dominio dado
Tipo de archivo:	Buscar un determinado tipo de archivo
título:	Buscar sitios con la(s) palabra(s) dada(s) en el título de la página
inurl:	Buscar sitios con la(s) palabra(s) dada(s) en la URL
en el texto:	Buscar sitios con la(s) palabra(s) dada(s) en el texto de la página
ancla:	Busque sitios que tengan la(s) palabra(s) dada(s) en enlaces que apuntan a ellos
cache:	Mostrar el caché más reciente de una página web
IP:	**Solo Bing:** encuentra resultados basados en una dirección IP determinada
linkfromdomain:	**solo Bing:** busca enlaces en el dominio dado

Funciones adicionales de Google

Herramientas de búsqueda: El botón "Herramientas" presenta una nueva fila de opciones, que permite acotar los resultados de la búsqueda. Una de las opciones más interesantes de esta función es el "Rango personalizado", que se puede utilizar para buscar dentro de un marco de tiempo determinado.

Google Imágenes: El servicio de búsqueda inversa de imágenes más potente. https://images.google.com/

Búsqueda de información archivada

Google y Bing: ambos motores de búsqueda ofrecen una vista en caché de los resultados

La Wayback Machine: http://archive.org/web/

Archivo hoy: http://archive.is/

Yandex

Yandex opera el motor de búsqueda más grande de Rusia con una participación de mercado de alrededor del 65%.

Operadores de búsqueda de Yandex

Ejemplo	Descripción
"vo * música"	Encuentre todos los resultados con cualquier palabra donde se encuentre el asterisco (*)
gato de Cheshire | sombrerero | Alice	Busque cualquier palabra en la consulta. esta consulta funciona para Google también
croquet + flamenco	Esta consulta exigiría que la página tenga la palabra flamenco, pero no croquet.
rhost:org.wikipedia.*	Búsqueda inversa de host
mimo:pdf	Buscar un tipo de archivo específico
!Curiouser !y !curiouser	Buscar varias palabras idénticas
Brilla brilla pequeña estrella	Excluir "estrella" de los resultados de búsqueda
idioma:es	Búsqueda restringida por idioma
fecha:200712*, fecha:20071215..20080101, fecha:>20091231	Búsqueda restringida por fecha o intervalo de fechas

Motores de búsqueda: otras alternativas

carrot2.org: Carrot2 es un motor de búsqueda de agrupamiento que agrupa los resultados de búsqueda en conjuntos de temas

www.exalead.com/search: Exalead funciona bien para encontrar documentos que contienen el término de búsqueda

millionshort.com: Million Short permite eliminar resultados, que enlazan con el millón de sitios web más populares

globalfilesearch.com: el sitio afirma haber indexado 243 terabytes de archivos almacenados en servidores FTP públicos

Shodan - https://www.shodan.io

Shodan es un motor de búsqueda para encontrar dispositivos y tipos de dispositivos conectados a Internet. Permite buscar cámaras web, enrutadores, dispositivos IoT/SCADA y más.

Filtros Shodan

Filtrar	Descripción
ciudad:	Buscar resultados en una ciudad determinada
país:	Buscar resultados en un país determinado (código de 2 letras)
Puerto:	Buscar un puerto o puertos específicos
nombre de host:	Buscar valores que coincidan con el nombre de host
red:	Busque una IP o subred determinada (p. ej.: 192.168.1.0/24)
producto:	Busque el nombre del software identificado en el banner
versión:	Buscar la versión del producto
sistema operativo:	Buscar un nombre de sistema operativo específico
título:	Buscar en el contenido extraído de la etiqueta HTML
html:	Buscar en el contenido HTML completo de los devueltos página

Redes sociales

Facebook

Barra de búsqueda: permite buscar todos los perfiles que se han creado utilizando una dirección de correo electrónico o un número de teléfono determinado.

ID de Facebook: el ID de usuario de Facebook se puede encontrar usando https://findmyfbid.com. Alternativamente, mientras está conectado a Facebook, el ID de usuario se puede encontrar en el código fuente HTML después de la etiqueta fb://perfil/.

Búsqueda de gráfico de Facebook

Resultado	Consulta
Lugares **Lugares visitados** **Lugares visitados recientemente** **Lugares registrados** **Lugares que gustan**	**/search/UserID/places /** search/UserID/places-visited /search/ UserID/recent-places-visited /search/UserID/ places-check-in /**search/UserID/places-liked**
Páginas que le gustan	**/buscar/IDUsuario/páginas-me gusta**
Fotos **Fotos de** **Fotos por** **Fotos que gustan** **Fotos comentadas**	**/search/UserID/photos /** **search/UserID/photos-of /search/** **UserID/photos-by /search/UserID/** **photos-liked /**search/UserID/photos- commented
Aplicaciones utilizadas	**/buscar/ID de usuario/aplicaciones**
Vídeos **Vídeos de** **Vídeos de** **Vídeos que han gustado** **Vídeos comentados**	**/search/UserID/videos /** **search/UserID/videos-of /search/** **UserID/videos-by /search/UserID/** **videos-liked /**search/UserID/videos- commented
Eventos **Eventos unidos en 2010**	**/search/UserID/events /** search/str/UserID/events-joined/2010/date/events/intersect/
Publicaciones **Posts etiquetados** **Publicaciones que han gustado** **Publicaciones por año**	**/search/UserID/stories-by /** search/UserID/stories-tagged /search/ UserID/stories-liked /search/UserID/ stories-by/2010/date/ stories/intersect
Amigos **Parientes** **Seguidores** **Grupos** **empleadores** **compañeros de trabajo**	**/búsqueda/ID de usuario/** **amigos /búsqueda/ID de usuario/** **parientes /búsqueda/ID de** **usuario/seguidores /búsqueda/** **ID de usuario/grupos /búsqueda/ID** **de usuario/empleadores /búsqueda/ID de usuario/empleados**
Me gusta de la página	/me gusta

Consultas adicionales de gráficos de Facebook se pueden encontrar en:

- https://inteltechniques.com/osint/menu.facebook.html http://researchclinic.net/graph.html

Operadores de búsqueda de Twitter

Operador	Buscar tuits…
búsqueda de twitter	Contiene "twitter" y "buscar". Este es el operador por defecto
"hora feliz"	Con la frase exacta "hora feliz"
amor u odio	Conteniendo "amor" u "odio" (o ambos)
raíz de cerveza	Contiene "cerveza" pero no "raíz"
#haiku	Con el hashtag "haiku"
de:alexiskold	Enviado desde el usuario "alexiskold"
a: techcrunch	Enviado al usuario "techcrunch"
@mashable	Usuario de referencia "mashable"
"hora feliz" cerca de: "san francisco"	Con la frase exacta "hora feliz" y enviado desde "san francisco"
cerca de:NYC dentro de:15mi	Enviado desde 15 millas de "NYC"
superhéroe desde:2010-12-27	Con "superhéroe" y enviado desde la fecha "2010-12-27" (año-mes-día)
ftw hasta:2010-12-27	Con "ftw" y enviado actualizado "2010-12-27"
filtro hilarante: enlaces	Conteniendo "hilarante" y enlazando a URLs
fuente de la noticia: "Twitter ligero"	Conteniendo "noticias" e ingresado a través de Twitter ligero
geocódigo:47.37,8.541,10km Enviado desde 10km de Zúrich	

Se pueden encontrar consultas adicionales de Twitter en:

- https://twitter.com/search-advanced
- https://inteltechniques.com/osint/twitter.html

Enumeración de usuarios de redes sociales

A través de diferentes funciones, es posible enumerar los usuarios registrados:

	Gorjeo	Facebook	Instagram	LinkedIn	Xing
Registro	X	X	X	X	X
Contraseña olvidada	X	X	X	X	X
Barra de búsqueda		X			

La función de olvido de contraseña de Facebook y Twitter también revela los dos últimos dígitos del número de teléfono móvil registrado. Esta información puede ser utilizada para futuras investigaciones.

Instrumentos	
Maltego	Maltego es un marco OSINT extremadamente poderoso, que cubre el reconocimiento personal y de infraestructura.
FOCA	FOCA es una herramienta que encuentra principalmente metadatos e información oculta en documentos escaneados. Estos documentos se pueden encontrar en páginas web y se pueden descargar y analizar con FOCA. (https://www.elevenpaths.com)
Técnicas Intel	Intel Techniques es una navaja suiza para OSINT https://inteltechniques.com
Robtex	Herramienta de Internet Robtex Swiss Army Knife. Robtex utiliza varias fuentes para recopilar información pública sobre direcciones IP, nombres de dominio, nombres de host, sistemas autónomos, rutas, etc. Los datos de acceso abierto se indexan y almacenan en una base de datos. https://www.robtex.com/

Enlaces adicionales

- **haveibeenpwned.com:** busca cuentas comprometidas
- **dnsdumpster.com:** busca hosts relacionados con un dominio
- **crt.sh:** busca en listas de transparencia de certificados

Libros

- **Google Hacking para Penetration Testers :** Johnny Long
- **Técnicas de inteligencia de código abierto :** Michael Bazzell
- **Privacidad y seguridad :** Michael Bazzell
- **Esconderse de Internet :** Michael Bazzell

www.compass-security.com