Webinar Gratuito

Google Hacking

V. 2

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Sábado 15 de Noviembre del 2014

¿Quién Soy?

- Consultor e Instructor Independiente en Hacking Ético, Informática Forense y GNU/Linux.
- Ex Integrante de RareGaZz y actual integrante de PeruSEC.
- Ex Redactor en la Revista Linux+ DVD (ES).
- Creador del II Reto Forense Digital Sudamericano - Chavín de Huantar 2012.
- Brainbench Certified Network Security (Master), Brainbench Certified Computer Forensics (U.S.) & Brainbench Certified Linux Administration (General).
- Más de 11 años de experiencia en el área.
- @Alonso_ReYDeS
- pe.linkedin.com/in/alonsocaballeroquezada/

Construir Consultas en Google

Reglas doradas para buscar en Google

1. Las consultas en Google no son sensibles a mayúsculas (Papas Fritas)

2. La única excepción es el operador (OR)

3. Los “comodines” en Google, representan una palabra en la frase de búsqueda (*)

4. Google se reserva el derecho de ignorarlo. (the, a, for)

Google

Búsqueda Básica

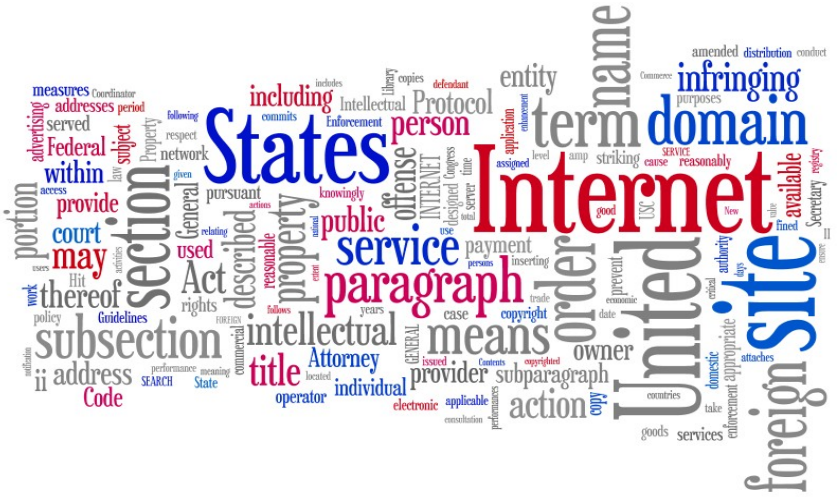
Buscar en Google es un proceso, el objetivo es encontrar información sobre un tópico. El proceso inicia con una búsqueda básica, la cual es modificada de diversas maneras hasta solo obtener páginas relevantes. Es raro que Google proporcione exactamente lo buscado en un solo intento.

La consulta más simple consiste de una sola palabra.

esteganografía

Una búsqueda más “compleja” sería la búsqueda de una frase.

“En un lugar de la mancha de cuyo nombre”
“En un primer momento dios creo”



Operadores Booleanos & Caracteres Especiales

Para realizar búsquedas avanzadas es necesario entender los operadores booleanos (AND, OR y NOT). También se pueden utilizar técnicas de agrupamiento que utilizan los paréntesis.

El operador Booleano más utilizado es AND. El cual se utiliza para incluir varios términos en la consulta.

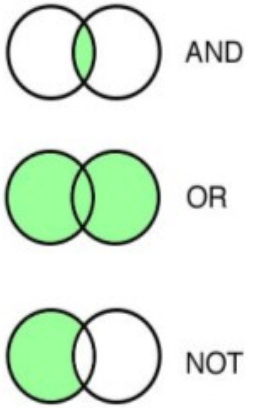
El símbolo (+) obliga la inclusión de la palabra que sigue. Sin espacio.

El operador NOT excluye una palabra de la búsqueda. Igual a (-)

Un operador poco común es OR. (|), el cual indica a Google incluir una palabra o la otra en la consulta.

intext:password | pass

intext:(password | pass)

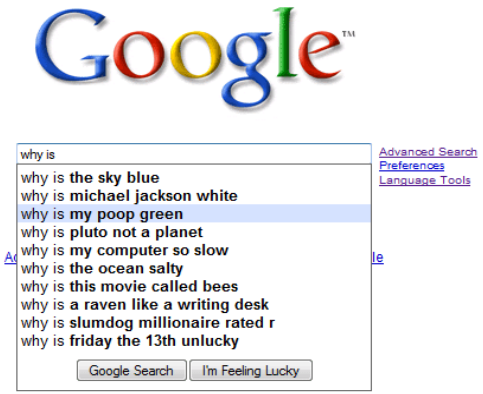


Reducir la Búsqueda

Para alcanzar la mayor cantidad de resultados relevantes, se necesita frecuentemente reducir la búsqueda, modificando la consulta original.

Aunque Google por defecto tiende a proporcionar resultados muy relevantes para las búsquedas más sencillas, es nuestra labor realizar búsquedas más complejas para obtener un subconjunto más explícito de sitios webs.

Casi todo el Google Hacking se enfoca en las técnicas de reducción y sugerencias, es por esto la importancia comprender lo básico de la reducción para las búsquedas.



Las URLs de Google

Sintaxis:

https://www.google.com/search?num=100&safe=off&site=&source=hp&q=esteganografia&oq=esteganografia

Más:

https://www.google.com/search?num=100&safe=off&q=richard+stallman&oq=richard+stallman&gs_l=serp.3..0l10.160285.162846.0.163071.16.9.0.3.3.0.364.915.2-2j1.3.0....0...1c.1.58.serp..10.6.928.aFVXt2MlBeg

num: Número de Resultados
safe: Filtro de contenido para adultos
q: Consulta Realizada.
oq: Consulta Original. Cuando se selecciona una Búsqueda sugerida por Google.

Operadores Avanzados

intitle: allintitle: Búsqueda dentro del título de una página.

intext: allintext: Ubica texto dentro del texto de una página.

inurl: allinurl: Encuentra texto en una URL.

site: Reduce la búsqueda a sitios específicos.

filetype: Busca por archivos de un tipo específico.

link: Busca páginas enlazando a cierta página.

info: Muestra información de resumen de Google.

related: Muestra sitios similares a una URL conocida.

cache: Muestra como la página la última vez que Google la indexó.

GHDB

Existen dos páginas principales donde se mantienen listados de búsquedas que permiten encontrar sistemas vulnerables. A las búsquedas individuales se le denomina un GoogleDork. Estas Bases de Datos contienen diferentes tipos de búsquedas, las cuales permiten encontrar varios tipos de defectos de seguridad y asuntos relacionados, utilizando únicamente Google.

- Advisories and Vulnerabilities
- Error Messages
- Files containing juicy info
- Files containing passwords
- Pages containing login portales
- Sensitive Directories
- Varios Online Devices
- etc.

HACKERS FOR CHARITY.ORG

GOOGLE HACKING-DATABASE

Hackers for Charity
GHDB - http://www.hackersforcharity.org/ghdb/
Exploit DataBase
GHDB - http://www.exploit-db.com/google-dorks/

Herramientas

SiteDigger v3.0

SiteDigger 3.0 realiza búsquedas en Google para encontrar vulnerabilidades, errores, configuraciones, información privada, y otra información de interés en los sitios webs.

Sitio Web:
http://www.mcafee.com/us/downloads/free-tools/sitedigger.aspx
* Goolag

GooScan

GooScan es una herramienta que automatiza las consultas contra el buscador de Google. Estas consultas están diseñadas para encontrar potenciales vulnerabilidades en las páginas webs. Es como un Escanner que nunca se comunica directamente con el servidor web objetivo, ya que todas las consultas son respondidas por Google, no por el objetivo.

Sitio Web: http://www.hackersforcharity.org/ghdb

Cursos Virtuales

Todos los Cursos están disponibles en Video.

Curso Virtual de Hacking Ético
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web
http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense
http://www.reydes.com/d/?q=Curso_de_Informatica_Forense

Más Información:


caballero.alonso@gmail.com

@Alonso_ReYDeS 


http://pe.linkedin.com/in/alonsocaballeroquezada/


ReYDeS


http://www.reydes.com

Demostraciones

Es momento de las demostraciones

Más Material

Videos de 22 Webinars Gratuitos que he dictado sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

http://www.reydes.com/d/?q=videos

Todas las diapositivas utilizadas en los Webinars Gratuitos las encuentran en la siguiente página.

http://www.reydes.com/d/?q=node/3

Todos los artículos y documentos que he publicado.

http://www.reydes.com/d/?q=node/2

Mi Blog sobre temas de mi interés.

http://www.reydes.com/d/?q=blog/1

Muchas Gracias

Google Hacking

V. 2

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Sábado 15 de Noviembre del 2014

Curso Online de Hacking Aplicaciones Web

Días:

Sábados 6, 13, 20 Julio y 3, 10 de Agosto del 2013.

Horario:

De 9:00am a 12:00 (UTC -05:00)

Más Información:

http://www.slideshare.net/reydes/curso-hacking-aplicacionesweb

Correo electrónico: caballero.alonso@gmail.com
Twitter: https://twitter.com/Alonso_ReYDeS
LinkedIn: http://pe.linkedin.com/in/alonsocaballeroquezada/
Skype: ReYDeS
Sitio Web: http://www.reydes.com