

# Google Hacking para Pentesters

*(Mas que una búsqueda, un conducto de intrusión)*



Por...

Eder A. López.

WSS

WhiteSec Sistemas  
dr.h47@live.com.mx  
www.whitesec.com.mx  
© 2010 – 2011

- 1\.** **Introducción.**
- 2\.** **¿Qué es un Pentester?**
- 3\.** **Antecedentes de Google Hacking.**
- 4\.** **Google Hacking, una técnica infalible de reconocimiento pasivo.**
- 5\.** **Poderes mágicos de Google Hacking.**
- 6\.** **Conociendo y practicando un poco.**
- 7\.** **Nota final.**
- 8\.** **Recursos para Google Hacking recomendados.**
- 9\.** **Lectura y recursos para la elaboración de este artículo.**
- 10\.** **Despedida.**

## 1\ **Introducción.**

Si, desde luego ya se que hay cientos de publicaciones navegando por la red sobre este tema, pero al igual he visto, lo que no se aborda en ellos, aparte de los términos no muy bien claros es una poca complejidad sobre esta técnica muy utilizada, pero poco conocida. Ya que se dice por ahí, que no es lo mismo manejar un auto que saberlo conducir, y lo mismo digo aquí, saber utilizar los parámetros avanzados de búsquedas de google, no nos convierte en *pentesters*, *analistas* y mucho menos en *hackers*.

Si bien es cierto en esta sencilla publicación orientado a pentesters, tratare de abordar de forma clara y precisa los conceptos y técnicas fundamentales que encierra esta técnica sin hacer de este escrito una publicación de muchas paginas y mucho menos aburrida. Pero antes, ya para ir entrando en materia conozcamos primero que es un *Pensester*.

## 2\ **¿Qué es un Pentester?**

En el campo de la informática y el análisis y protección de datos, el Pentester, Security Tester, White Security Tester, o como se le quiera llamar. Para muchos es un Hacker, cosa que si adopta cierto perfil pero no es un hacker, más bien considero, es un usuario poco avanzado o experto con ciertos conocimientos en materia de seguridad informática, en el análisis y protección de datos, un poco curioso con amplias habilidades de análisis, concentración y de aprendizaje que se interesa por la seguridad informática, pero como todo, no todo lo que sea blanco es pureza. Así también los hay BlackTesters, o BST (Black Security Testers), pero por ahora no hablare de ellos.

## 3\ **Antecedentes de Google Hacking.**

Para ir entrando en materia, siempre digo, que conocer nuestras raíces, nos ayuda a conocernos y a hacer de nuestra personalidad, algo más atractivo, interesante y culto, por lo tanto conozcamos las raíces de google hacking y por si fuera poco al padre de esta técnica.

GooHack o Google Hacking, es lo que algunos llaman *PEBAG* (*Parámetros Especiales de Búsqueda Avanzada de Google*), y fue dada a conocer en *DefCon XI*, una de las reuniones mas importantes de Seguridad Informática celebradas en Latinoamérica mediante una charla presentada por Johnny Long a quien se le conoce como el padre de *Google Hacking*.

#### **4\ Google Hacking, una técnica infalible de reconocimiento pasivo.**

Google Hacking nos es más que una técnica de fusión basada en el uso malicioso de parámetros especiales de google, con el fin de conseguir búsquedas avanzadas y precisas, cuyo afán es obtener datos sensibles que pudiesen ver afectados a personas particulares, empresas públicas o privadas.

En la actualidad como se había de esperar, tal como y para lo que fue presentado en sus inicios, ha seguido siendo una herramienta infalible de reconocimiento pasivo en la caja de técnicas de los analistas de seguridad, pentesters y demás categorías de expertos, y otros por ahí que también la usan pero que de seguro solo ven una técnica nueva y la están metiendo en google sin si quiera saber de que se trata, ni para que sirve, sus fines o beneficios.

#### **5\ Poderes mágicos de Google Hacking.**

Esta técnica posee poderes tan secretos, mágicos y complejos, tanto así que con tan solo hacer simples consultas a través del buscador de google, podemos conseguir información sensible suficiente sobre un objetivo, como, archivos de configuración, paneles de servidores, puntos de acceso, claves y contraseñas de sistemas, ver videos privados, datos personales, números telefónicos, e-mails, hashes, errores de programación, y algo para lo que mas a sido utilizado es la búsqueda de puntos vulnerables para inyección de código arbitrario.

Pero como todo, tiene sus límites, esta vez el límite dependerá de la creatividad y el ingenio del usuario atacante, analista o un usuario común ya que dependiendo de nuestra creatividad, combinada con esta técnica podríamos conseguir cosas como:

- Datos de configuración de servidores Web y de redes.
- Datos de acceso a bases de datos.
- Mensajes y advertencias de errores de programación.
- Datos personales, o sensibles de alguna compañía.
- Búsquedas aleatorias de Victimas de Hacking.
- Números y claves de tarjetas de crédito.
- Claves y cuentas de correo.
- Acceso a archivos logs.
- Datos específicos de Sistemas Operativos.
- Bases de datos de usuarios y contraseñas.

- Puntos de acceso a paneles de administración de servidores Web.
- Consultas y mapeado de servidores.

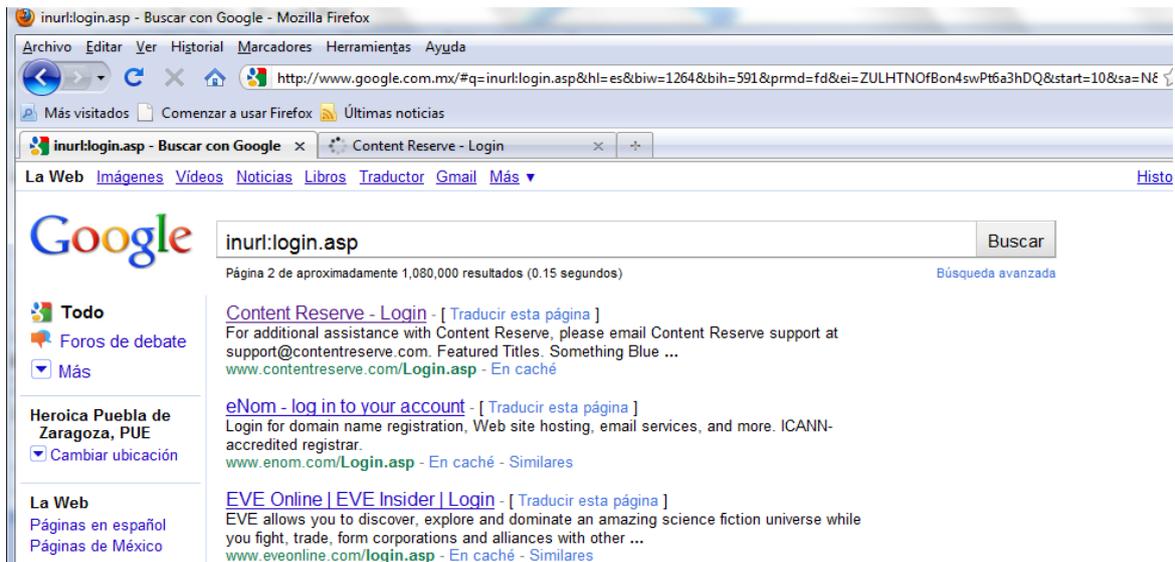
Podría escribir más y más cosas, pero como digo, esto dependerá de la creatividad del analista o atacante, y bueno yo por el momento no estoy muy creativo.

Además de eso, no quiero que este artículo sea muy extenso, por lo tanto no voy a mencionar todos los parámetros y formas de búsqueda, pero si los parámetros más utilizados por los pentesters, que con ese fin fue pensado este artículo.

**Nota:** Los demás parámetros especiales y formas de búsqueda de Google Hacking que no se mencionen aquí se podrán encontrar en un libro escrito por el mismo Johnny Long, el cual mencionare en la sección Referencias, luego podéis buscarlo por la red y al mismo tiempo empezar a practicar Google Hacking.

## 6). Conociendo y practicando un poco.

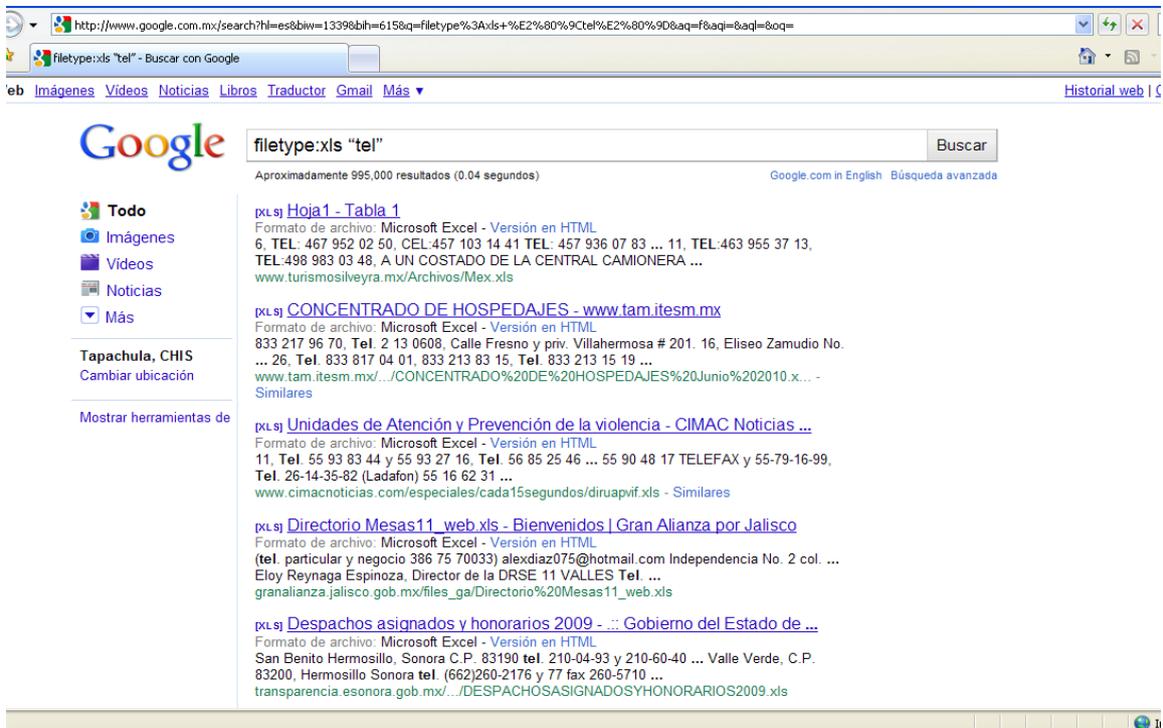
PARAMETRO	MODO DE EJECUCIÓN	DETALLES
inurl	inurl:login.asp	<p>Busca el directorio compuesto de login.asp que se encuentre como parte de la URL, por medio del cual podremos acceder a los recursos administrativos del sistema a nivel Web en este caso.</p> <p>Además podemos intercambiar las búsquedas y en vez de login.asp podemos poner algo como: admin.asp, password, etc.</p> <p>En fin esto dependerá de la creatividad y el ingenio del pentester.</p>



filetype filetype:xls "tel"

Es un operador que nos permite hacer búsqueda de ficheros con extensiones específicos. Por ejemplo en el ejemplo le estamos diciendo que busque archivos de Excel (.xls) que hagan referencia a la palabra "tel", o sea teléfonos, o también para buscar contraseñas.

Esto depende que tipo de fichero queremos buscar, podemos usar de todo tipo de extensiones por ejemplo: pl, mp3, txt, mdb, sql, php, asp, php, sh, etc.



link

link: whitesec.com.mx

Este operador muestra todos los sitios web que en sus paginas tengan links que apunten hacia mi blog [www.whitesec.com.mx](http://www.whitesec.com.mx), con esto al hacer un pentest podríamos saber la relación de la empresa que estemos testeando, ya sea con posibles proveedores, ventas online, socios, publicidades, hasta blogs personales o fotografías.

The screenshot shows a Google search interface. The search bar contains the query "link: whitesec.com.mx". The search results are displayed below the search bar, showing several entries from "WhiteSec Sistemas". The first entry is dated 8 Dec 2010 and mentions a link to a page on whitesec.com.mx. The second entry is dated 7 Dec 2010 and mentions a page about vulnerabilities in Arnet-WiFi modems. The third entry is dated 1 Nov 2010 and mentions a page about importing WordPress to Blogger. The fourth entry is dated 11 Abr 2011 and mentions a PDF file of basic Linux commands. The fifth entry is dated 23 Sep 2010 and mentions a PDF file about surviving without antivirus. The search results are displayed in a list format with blue links and black text. The Google logo is visible on the left side of the page. The search bar is located at the top of the page, and the search results are displayed below it. The search bar contains the query "link: whitesec.com.mx" and a "Buscar" button. The search results are displayed in a list format with blue links and black text. The search results are displayed in a list format with blue links and black text.

author

author: eder A. López

Esto hara una búsqueda en google por todos sitios, foros, blogs, en la cual haya comentado e iniciado un tema el usuario: Dr. H47.

The screenshot shows a Google search results page for the query "author: eder A. López". The search bar at the top contains the text "author: eder A. López" and a "Buscar" button. Below the search bar, it indicates "Aproximadamente 424,000 resultados (0.21 segundos)". The left sidebar contains navigation options: "Todo", "Imágenes", "Videos", "Noticias", "Más", "Tapachula, CHIS", "Cambiar ubicación", "Todos los resultados", "Sitios con imágenes", "Orden cronológico", and "Más herramientas". The main content area displays several search results:

- Browsing by Author López Bautista, Eder Santiago - Repositorio ...**  
Issue Date, Title, Author(s). Nov-2007. Análisis de la calidad del transporte de potencia - López Bautista, Eder Santiago ...  
[bibdigital.epn.edu.ec/browse?type=author...López..Eder... - En caché](#)
- Facebook | Eder Lopez | Facebook**  
Eder Lopez is on Facebook. Únete a Facebook para conectarte con Eder Lopez y otras personas que tal vez conozcas. facebook da el poder a la gente de acceder ...  
[es-es.facebook.com/metalirintzi - En caché](#)
- Introducción a C++ para principiantes**  
Formato de archivo: PDF/Adobe Acrobat - Vista rápida  
Eder A. López. 2010 - 2011. WhiteSec Sistemas [www.whitesec.com.mx](#) dr.h47@live.com.mx ..... Author: Dr. H47. Web Site: [http://www.whitesec.com.mx/...www.whitesec.com.mx/papers/Introduccion-a-C++-para-principiantes.pdf](#)
- Usando colores en nuestros programas de C++**  
Formato de archivo: PDF/Adobe Acrobat - Vista rápida  
Usando colores en nuestros programas de C++. Por... Eder A. López. WhiteSec Sistemas [www.whitesec.com.mx](#) dr.h47@live.com.mx. Marzo de 2011. ...  
[www.whitesec.com.mx/.../Usando-colores-en-nuestros-programas-de-C++.pdf](#)
- Simulando una clave de acceso en C++**  
9 Ene 2011 ... Eder A. Lopez dr.h47@live.com.mx. Powered by Dr. H47 ++++++. Code in C : Sagrini 2010 : [elhacker.net \\*/ #include <stdio.h> ...foro.elhacker.net/.../simulando\\_una\\_clave\\_de\\_acceso\\_en\\_c-1316200.0.html - En caché](#)
- Eder Lopez (music) | Free Music, Tour Dates, Photos, Videos**  
Eder Lopez (music)'s official profile including the latest music, albums, songs, music videos and more updates.  
[www.musica.com/ederlopezmusica - En caché](#) Similar...

site

site:whitesec.com.mx  
'hacking'

Esto buscara dentro de whitesec.com.mx y mostrara todos los enlaces donde encuentre la palabra 'hacking'.

Aquí en este ejemplo en vez de doble comilla puse una simple, eso hace mas especifica aun la búsqueda, será cuestión de cada uno seguir optimizando los métodos.

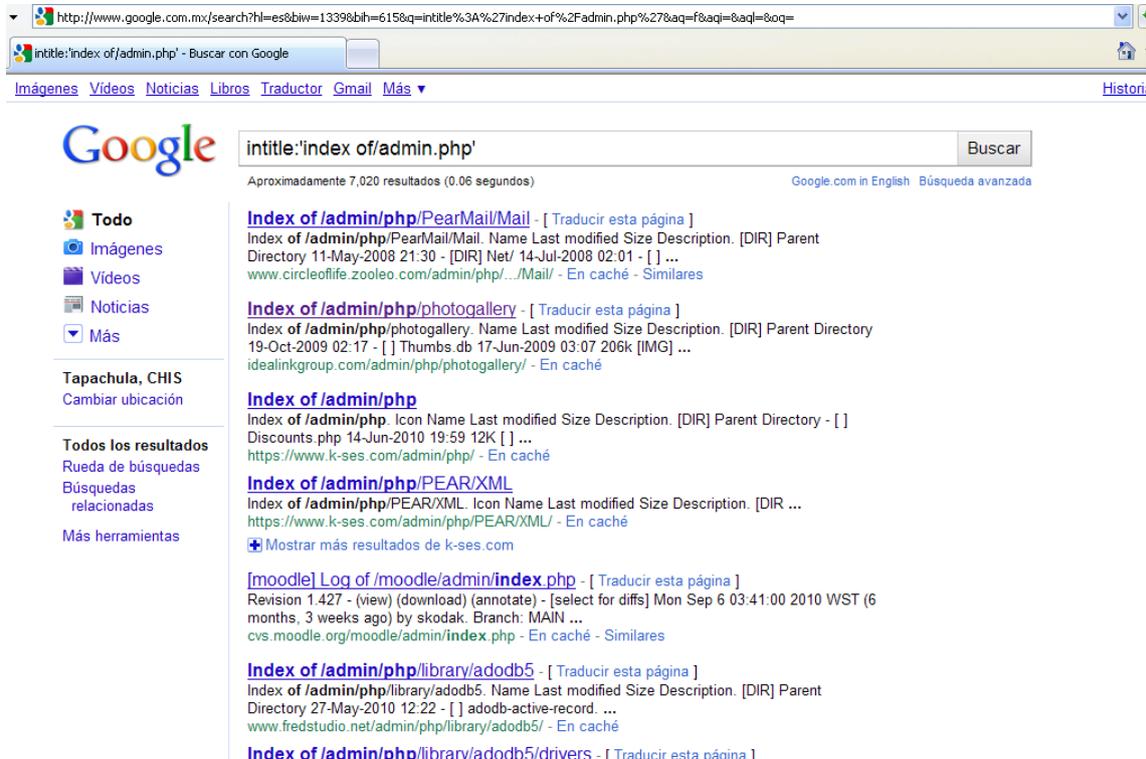
Este parámetro puede usarse para encontrar palabras clave dentro del sitio al que estamos haciendo pentest.

The screenshot shows a Google search interface. The search bar contains the query 'site:whitesec.com.mx 'hacking'' and the search button is labeled 'Buscar'. Below the search bar, it indicates 'Aproximadamente 153 resultados (0.05 segundos)'. The search results are listed on the right side of the page, with a left sidebar containing navigation options like 'Todo', 'Imágenes', 'Videos', 'Noticias', 'Blogs', 'Libros', 'Foros de debate', and 'Más'. The search results include several entries from 'WhiteSec Sistemas' with dates and titles such as 'Hacking - In(Seguridad) | WhiteSec Sistemas', 'X.25 Ethical Hacking Conferences 2011 | WhiteSec Sistemas', 'Eventos | WhiteSec Sistemas', '2011 enero | WhiteSec Sistemas', 'Token RSA atacada por hackers | WhiteSec Sistemas', and '2011 abril 10 | WhiteSec Sistemas'. Each result includes a brief description and a link to the full article.

intitle

intitle:'index  
of/admin.php'

Esto busca en el título de una página web. Es útil para buscar directorios predefinidos en los servidores.



Esto apenas es una muestra de los operadores de búsqueda más usados, y hay muchos mas que ya por su propia cuenta en interesado irá descubriendo, al igual como había dicho antes, esta técnica de reconocimiento pasivo se limita, a la curiosidad, lógica y el ingenio del pentester, ya que por medio de esta técnica haciendo combinaciones elegantes podemos conseguir cosas tan precisas en pocos segundos. Antes de terminar veamos cómo podemos usarlo.

### Antes las mismas funciones podemos usarlas con el parámetro (all)

all

all operador

Ejemplos:

allinurl

allfiletype

allintitle

El parámetro all hace referencia a todo, es decir hacer una búsqueda profunda, por lo que al usar el parámetro all se hace un escaneo mas a fondo por lo cual tendríamos posibilidades de encontrar más cosas.



allinurl all inurl:login.asp Esto buscara ficheros login.asp de  
intitle:intranet site:com acceso a intranets.

The screenshot shows a Google search interface. The search bar contains the query "all inurl:login.asp intitle:intranet site:com". The search results are displayed on the right side of the page. The first result is "LCI Intranet Login - ©Leader Communications Inc" with a link to "https://www.lcibest.com/LCI/login.asp". The second result is "Healthcare Services Group, Inc. :: Intranet" with a link to "intranet.hcsgcorp.com/login.asp". The third result is "Intelligent Evolution (IE) - Intranet Login" with a link to "www.intellivolve.com/Intranet/login.asp". The fourth result is "Google Apps (for business) OpenID login for ASP.NET intranet site ..." with a link to "www.techques.com/.../Google-Apps-(for-business)-OpenID-login-for-ASP.NET-intranet-site". The fifth result is "INTEGRA INTERNATIONAL - Members Intranet & Productivity Tool" with a link to "integra-international.webexone.com/login.asp".

site site:presidencia.gob.m Buscara todo lo que tenga que ver  
x fraude con fraudes alojado en  
presidencia.gob.mx

The screenshot shows a Google search interface. The search bar contains the query "site:presidencia.gob.mx fraude". The search results are displayed on the right side of the page. The first result is "Atrapan a falsa funcionaria del Invi por presunto fraude" with a link to "www.presidencia.gob.mx/prensa/ultimasnoticias/?contenido...". The second result is "El gobierno de EUA extradita a un fugitivo de la ley mexicana ..." with a link to "www.presidencia.gob.mx/prensa/pgpr/?contenido=36276". The third result is "México - Presidencia de la República" with a link to "ehecat1.presidencia.gob.mx/prensa/sfp/?contenido...true". The fourth result is "Gobierno Federal | Presidencia de la República | México | El ..." with a link to "www.presidencia.gob.mx/index.php?DNA=85...1...". The fifth result is "Imprimir - México - Presidencia de la República | Las Buenas ..." with a link to "fox.presidencia.gob.mx > ... > Seguridad". The sixth result is "México - Presidencia de la República | México" with a link to "www.presidencia.gob.mx/mexico/sabiasque/?contenido...". The seventh result is "La cooperación internacional en materia de justicia rinde frutos ...".

site

site:whitesec.com.mx  
filetype:pdf

Buscara en whitesec.com.mx todos los ficheros .pdf alojados en el servidor.

The screenshot shows a Google search interface. The search bar contains the query "site:whitesec.com.mx filetype:pdf" and the search button is labeled "Buscar". Below the search bar, it indicates "10 resultados (0.06 segundos)" and "Google.com in English Búsqueda avanzada".

On the left side, there is a navigation menu with the following items: "Todo", "Imágenes", "Videos", "Noticias", "Más", "Tapachula, CHIS", and "Cambiar ubicación".

The search results list the following items:

- Informática básica I**  
Formato de archivo: PDF/Adobe Acrobat - Vista rápida  
INFORMÁTICA BÁSICA I. PRESENTA. Eder A. López. [White Security Group] www.whitesec.com.mx dr.h47@live.com.mx. © 2010 - 2011 White Sec Team. ...  
www.whitesec.com.mx/papers/Informatica\_basica.pdf
- Sobreviviendo sin Antivirus.**  
Formato de archivo: PDF/Adobe Acrobat - Vista rápida  
Sobreviviendo sin Antivirus. (Consejos y trucos). Por... Eder A. López. White Sec Team  
www.whitesec.com.mx dr.h47@live.com.mx. [ White Security Group ] ...  
www.whitesec.com.mx/papers/Sobreviviendo-sin-Antivirus.pdf
- Leer y escribir una cadena de caracteres con gets y puts**  
Formato de archivo: PDF/Adobe Acrobat - Vista rápida  
Leer y escribir una cadena de caracteres con gets y puts. Por. Eder A. López. White Security Group www.whitesec.com.mx dr.h47@live.com.mx ...  
www.whitesec.com.mx/papers/caracteres-con-gets-puts.pdf
- Comandos básicos de linux.**  
Formato de archivo: PDF/Adobe Acrobat - Vista rápida  
Comandos básicos de linux. Por... Eder A. López. WhiteSec Sistemas dr.h47@live.com.mx -  
www.whitesec.com.mx. Febrero de 2011. ...  
www.whitesec.com.mx/papers/comandos-basicos-de-linux.pdf
- Introducción a C++, para principiantes.**  
Formato de archivo: PDF/Adobe Acrobat - Vista rápida  
Introducción a C++, para principiantes. Por... Eder A. López. 2010 - 2011. WhiteSec Sistemas  
www.whitesec.com.mx dr.h47@live.com.mx. Marzo de 2011. ...  
www.whitesec.com.mx/papers/Introduccion-a-C++-para-principiantes.pdf

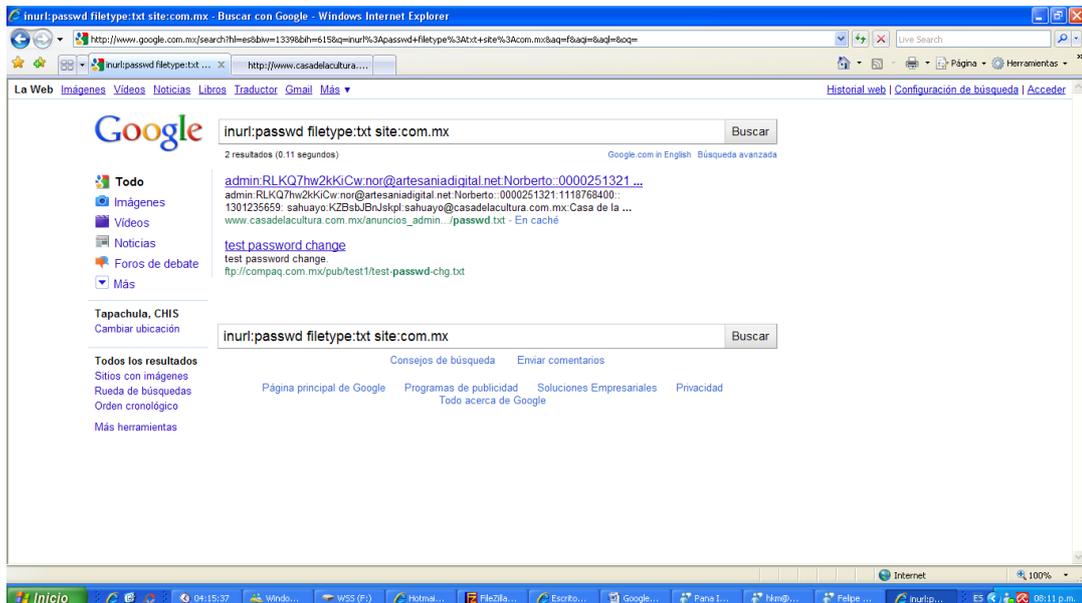
At the bottom of the visible results, there is a partial entry: "Infección viral, mediante el registro de Windows".

site  
inurl  
filetype

site:whitesec.com.mx  
inurl:passwd  
filetype:log

Esto buscara dentro de  
whitesec.com.mx en el directorio  
passwd el log de contraseñas.

También se puede usar así:  
inurl:passwd filetype:txt  
site:com.mx



## 7\). **Nota final.**

Para profundizar más vuestro conocimiento en el hacking con google, recomiendo:

- Buscar en google términos como “google dorks”.
- Leer sobre configuraciones de bases de datos y directorios de servidores.
- Leer el libro “Google Hacking for Penetration Tester”, de Johnny Long. Se puede conseguir en cualquier parte de google, o pídanmelo via E-mail.
- Leer la versión en español de “El Arte de la Intrusión”, de Kevin Daniel Mitnick. Igual se puede encontrar en google, o pídanmelo via E-mail.
- Y claro los más importantes, lectura, curiosidad, imaginación y pasión por el arte. Y sobre todo no usar estos conocimientos con fines maliciosos o con intención de dañar a terceras personas.

## 8\). **Recursos para Google Hacking recomendados.**

- “Google Hacking for Penetration Tester”, by Johnny Long.
- “El Arte de la Intrusión”, de Kevin Daniel Mitnick.
- “The Art Of Deception”, igual de Kevin Daniel Mitnick.
- “Goolag\_Scanner\_1.0.0.40\_Setup.exe”, Tool con cientos de dorks para hacer penetration tester.
- “NMAP a Security Auditing Tool”, es una presentación en ingles sobre el uso de NMAP.
- Parámetros especiales de búsquedas avanzadas de google.  
[http://www.googleguide.com/advanced\\_operators.html](http://www.googleguide.com/advanced_operators.html)
- Charla de Johnny Long en DefCon XI.  
<http://www.defcon.org/html/defcon-11/defcon-11-speakers.html#Long>
- “Optimización de búsquedas en Windows Vista”. By Eder A. López. Alojado en el blog en la sección ARTICULOS.

## 9\). **Lectura y recursos para la elaboración de este artículo.**

- “Google Hacking for Penetration Tester”, by Johnny Long.
- “El Arte de la Intrusión”, de Kevin Daniel Mitnick.
- “Goolag\_Scanner\_1.0.0.40\_Setup.exe”.
- Parámetros especiales de búsquedas avanzadas de google.  
[http://www.googleguide.com/advanced\\_operators.html](http://www.googleguide.com/advanced_operators.html)
- Charla de Johnny Long en DefCon XI.  
<http://www.defcon.org/html/defcon-11/defcon-11-speakers.html#Long>

## 10\). **Despedida.**

Solo mencionar que esto solo ha sido una introducción al Pentesting White, y que deseo que los que lean este artículo se aventuren a investigar más sobre esta técnica de reconocimiento pasivo y se vuelvan expertos en seguridad informática.

Al final también solo agregar un saludo a mis más grandes amigos que por ciertas razones, retirados, casados, divorciados o por cuestiones de trabajo ya casi no los veo, les dejo un afectuoso saludo.

Basshettzx ~ brainvirz ~ CaZs ~ kdx-tux ~ Cygog ~ dangus92 ~ Dedalo ~ Felipe ~ judg3 ~ KuTeR ~ Khronos ~ krisium ~ Molder ~ Pana\_Infierno ~ Shadinessdark ~ Tr4\$h ~ Vicent0! ~ Xianur0 ~ XcryptOR ~ Zero Bits.

Y en especial a mis preciados amigos del Team WhiteSec Argentina. Que podéis encontraros aquí: [www.whitesec.org](http://www.whitesec.org)

---

Venezuela ~ España ~ Colombia ~ Rusia ~ Ecuador ~ México  
~ Chile ~ Argentina ~ Paraguay ~ Perú ~ Salvador

Dr. H47  
**WhiteSec Sistemas.**  
© 2010 – 2011  
[www.whitesec.com.mx](http://www.whitesec.com.mx)  
[dr.h47@live.com.mx](mailto:dr.h47@live.com.mx)  
Abril 21 de 2011.

###

**TH3 3ND**