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

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 injección 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.

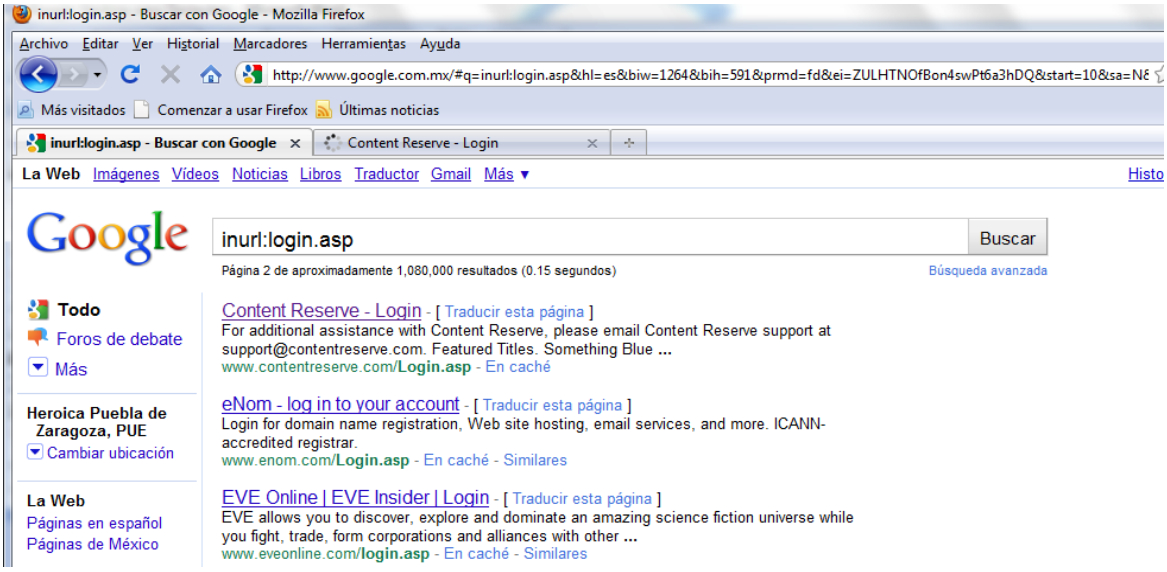
Podría escribir más y más cosas, pero como digo, esto dependerá de la creatividad del analista o atacante, y bueno yo por el momento no estoy muy creativo.

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.

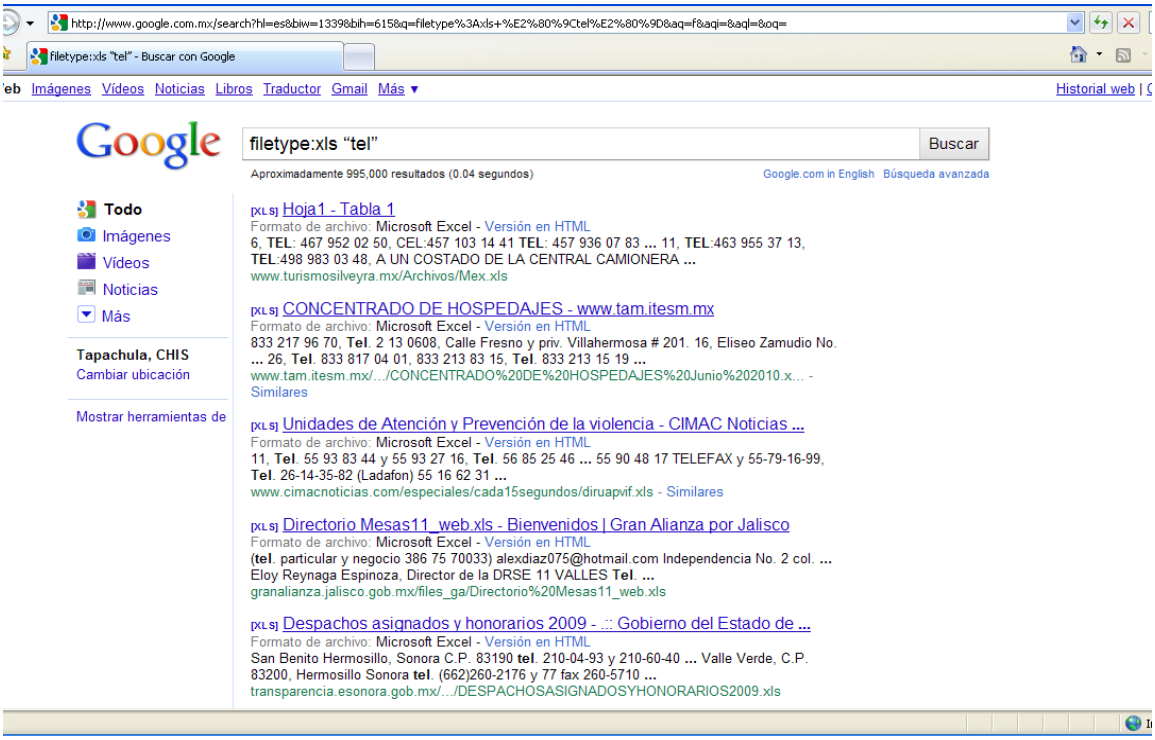
Nota: Los demás parámetros especiales y formas de búsqueda de Google Hacking que no se mencionen aquí se podrán encontrar en un libro escrito por el mismo Johnny Long, el cual mencionare en la sección Referencias, luego podéis buscarlo por la red y al mismo tiempo empezar a practicar Google Hacking.

6\. Conociendo y practicando un poco.

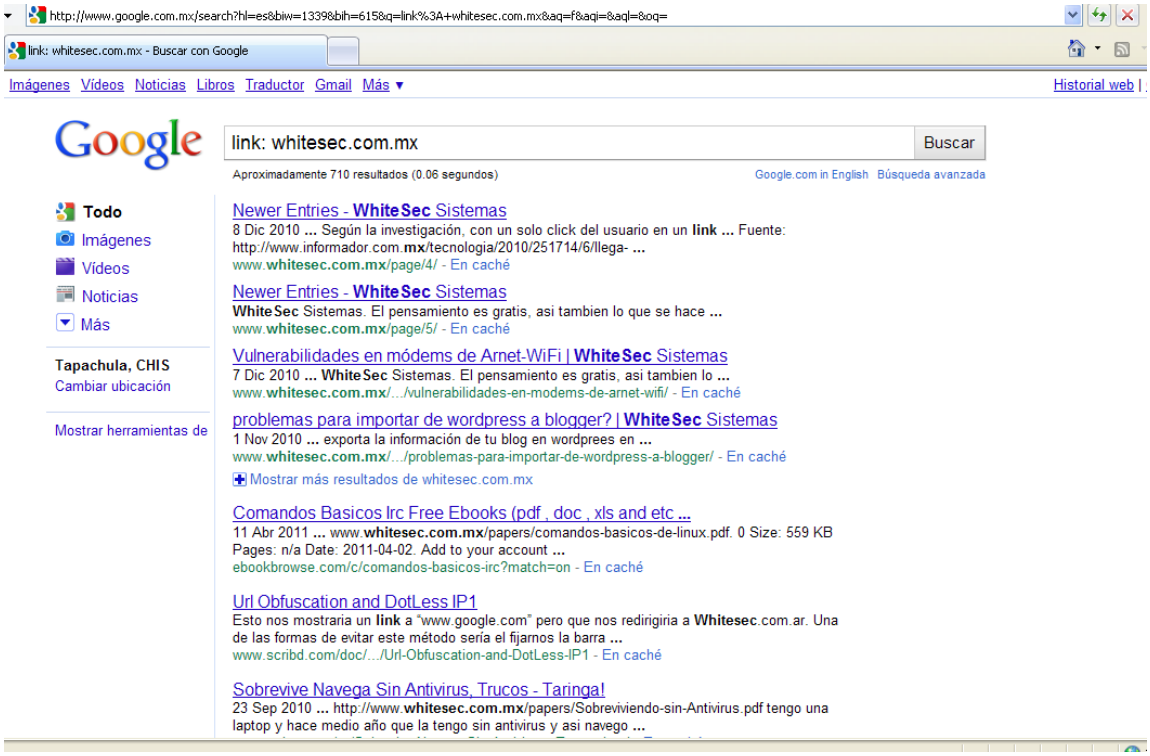
PARAMETRO	MODO DE EJECUCIÓN	DETALLES
inurl	inurl:login.asp	Busca el directorio compuesto de login.asp que se encuentre como parte de la URL, por medio del cual podremos acceder a los recursos administrativos del sistema a nivel Web en este caso. Además podemos intercambiar las búsquedas y en vez de login.asp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



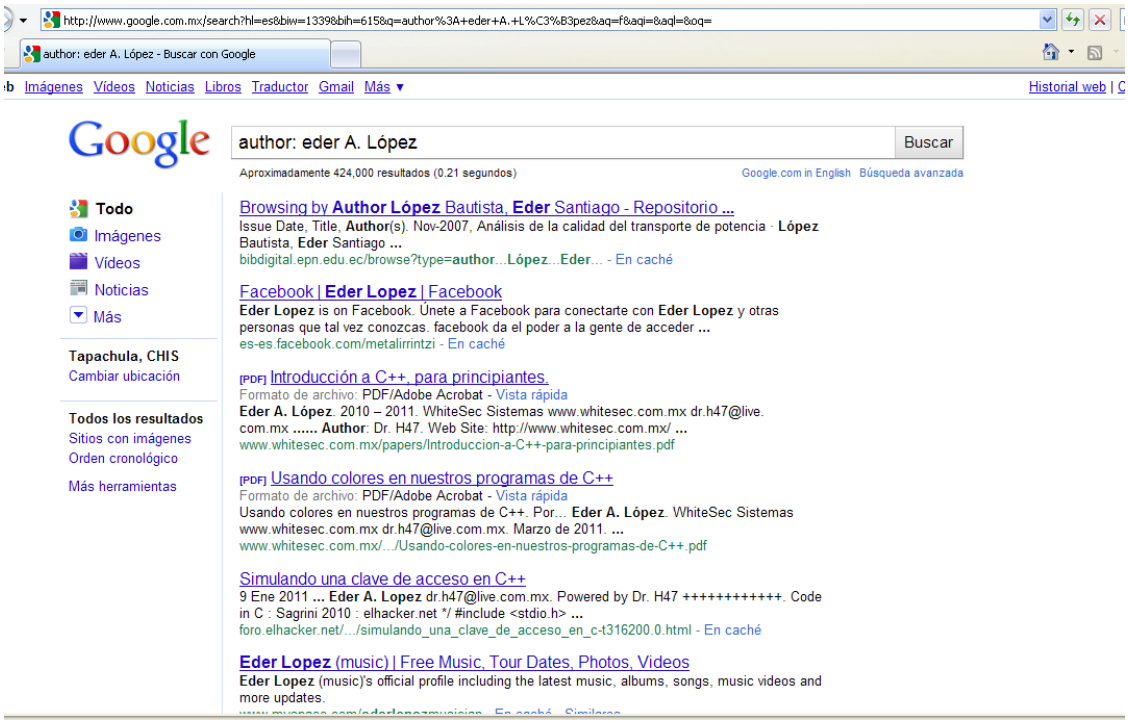
filetype	filetype:xls “tel”	Es un operador que nos permite hacer búsqueda de ficheros con extensiones específicos. Por ejemplo en el ejemplo le estamos diciendo que busque archivos de Excel (.xls) que hagan referencia a la palabra “tel”, o sea teléfonos, o también para buscar contraseñas. Esto depende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



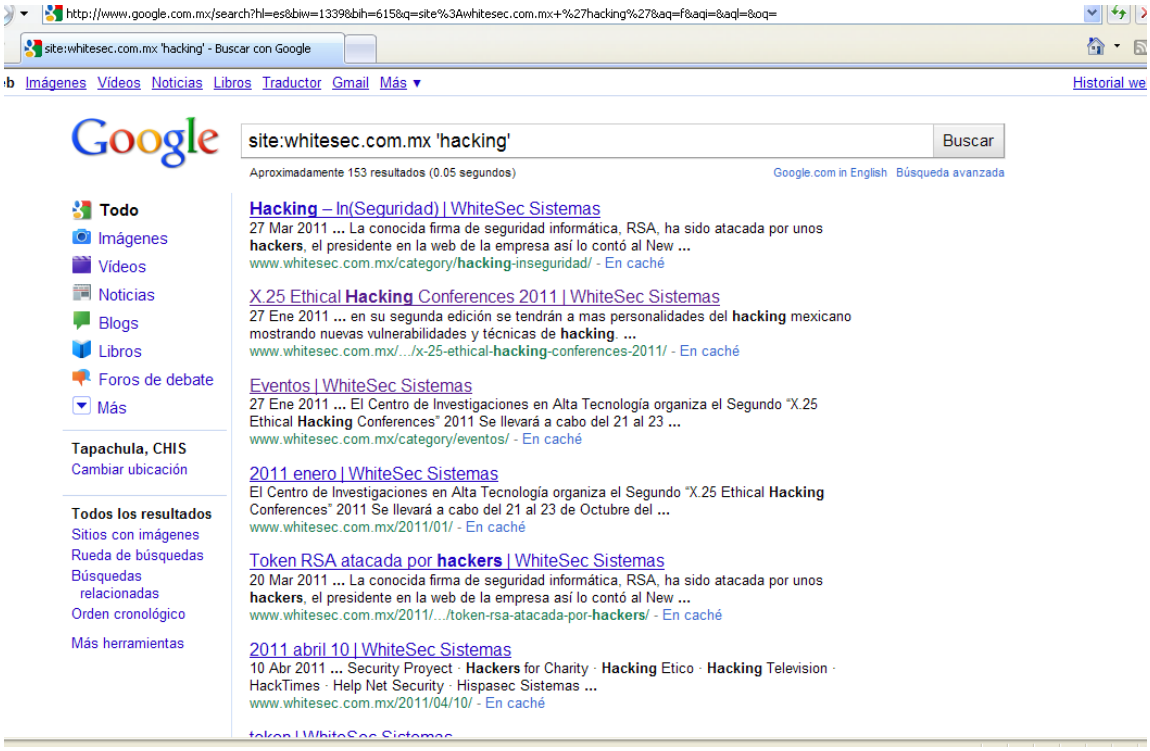
link	link: whitesec.com.mx	Este operador muestra todos los sitios web que en sus paginas tengan links que apunten hacia mi blog www.whitesec.com.mx, con esto al hacer un pentest podríamos saber la relación de la empresa que estemos testeando, ya sea con posibles provedores, ventas online, socios, publicidades,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



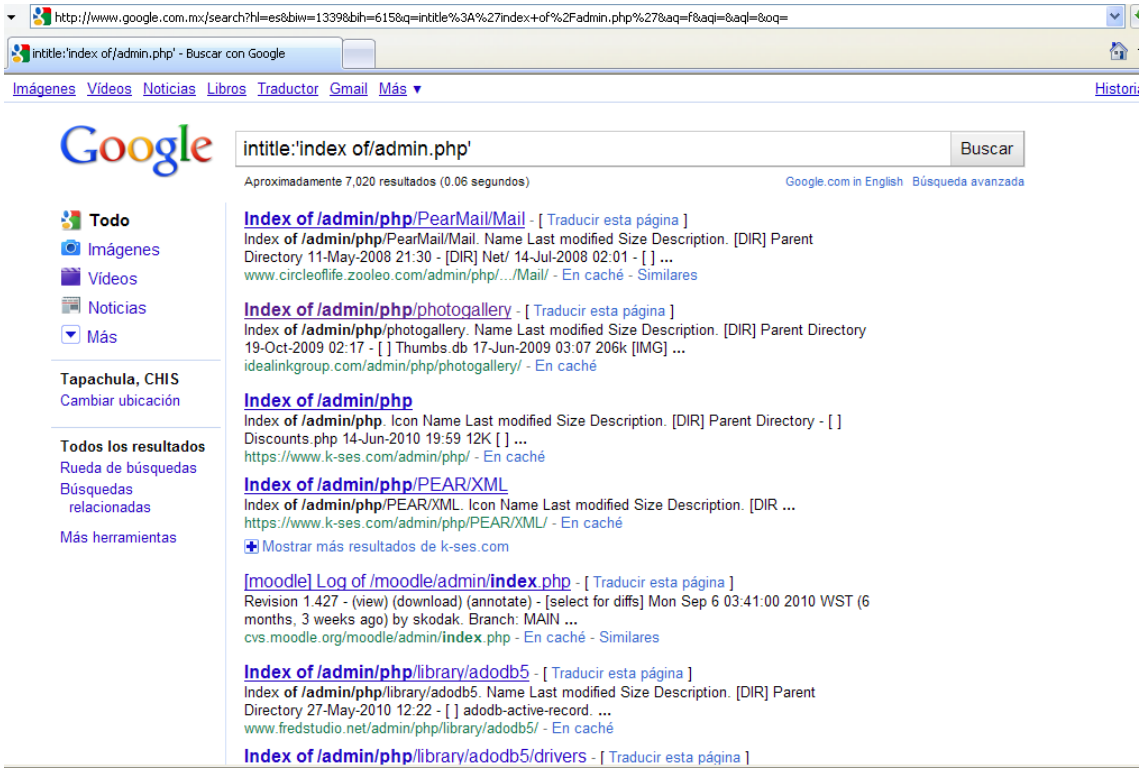
author	author: eder A. López	Esto hara una búsqueda en google por todos sitios, foros, blogs, en la cual haya comentado e iniciado un tema el usuario: Dr. H47.



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.



intitle	intitle:'index of/admin.php'	Esto busca en el titulo de una página web. Es útil para buscar directorios predefinidos en los servidores.

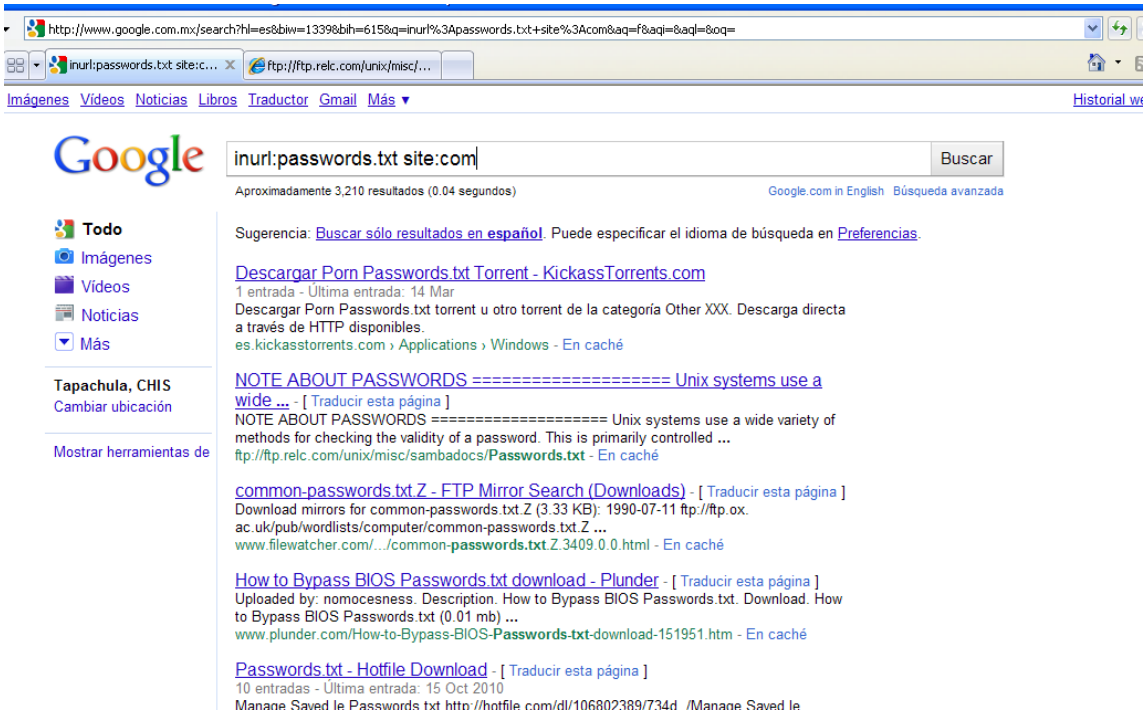


Esto apenas es una muestra de los operadores de búsqueda más usados, y hay muchos mas que ya por su propia cuenta en interesado irá descubriendo, al igual como había dicho antes, esta técnica de reconocimiento pasivo se limita, a la curiosidad, lógica y el ingenio del pentester, ya que por medio de esta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

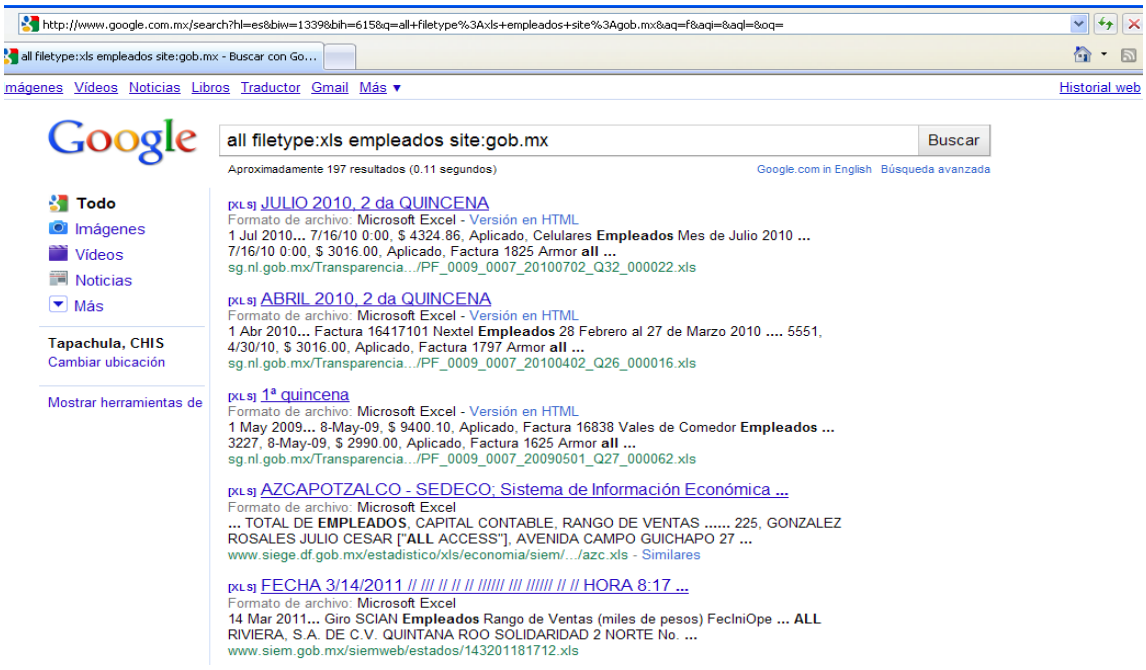
Antes las mismas funciones podemos usarlas con el parámetro (all)

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.

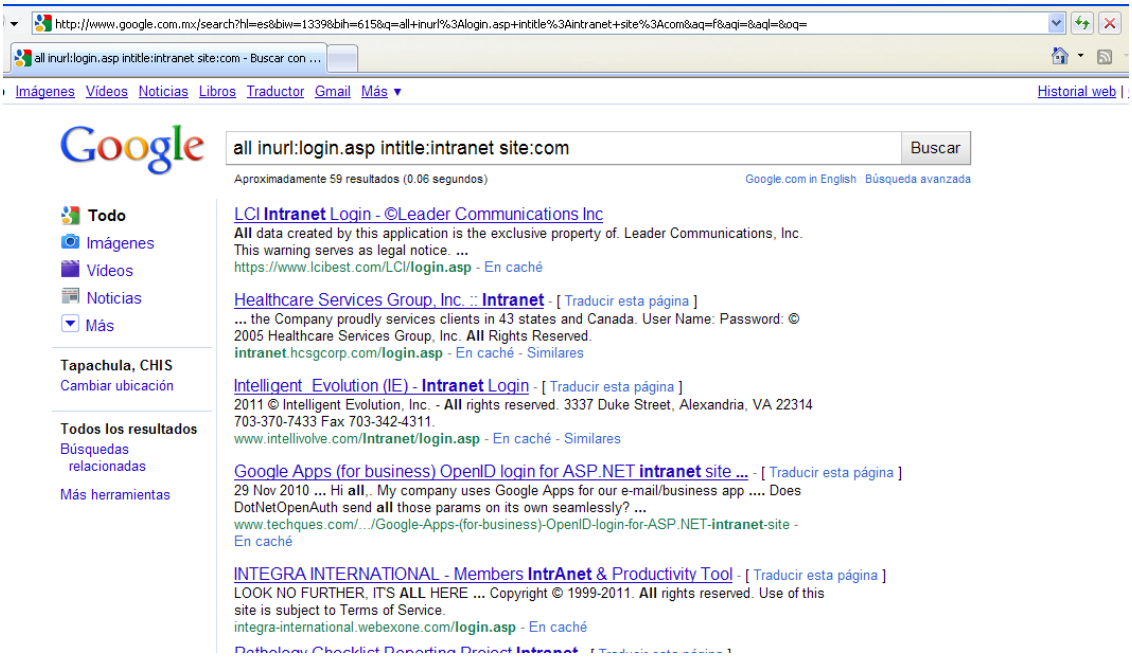
allinurl	inurl:passwords.txt site:com	Esto buscara el fichero passwords.txt dentro de todos los sitios .com que logre escanear.



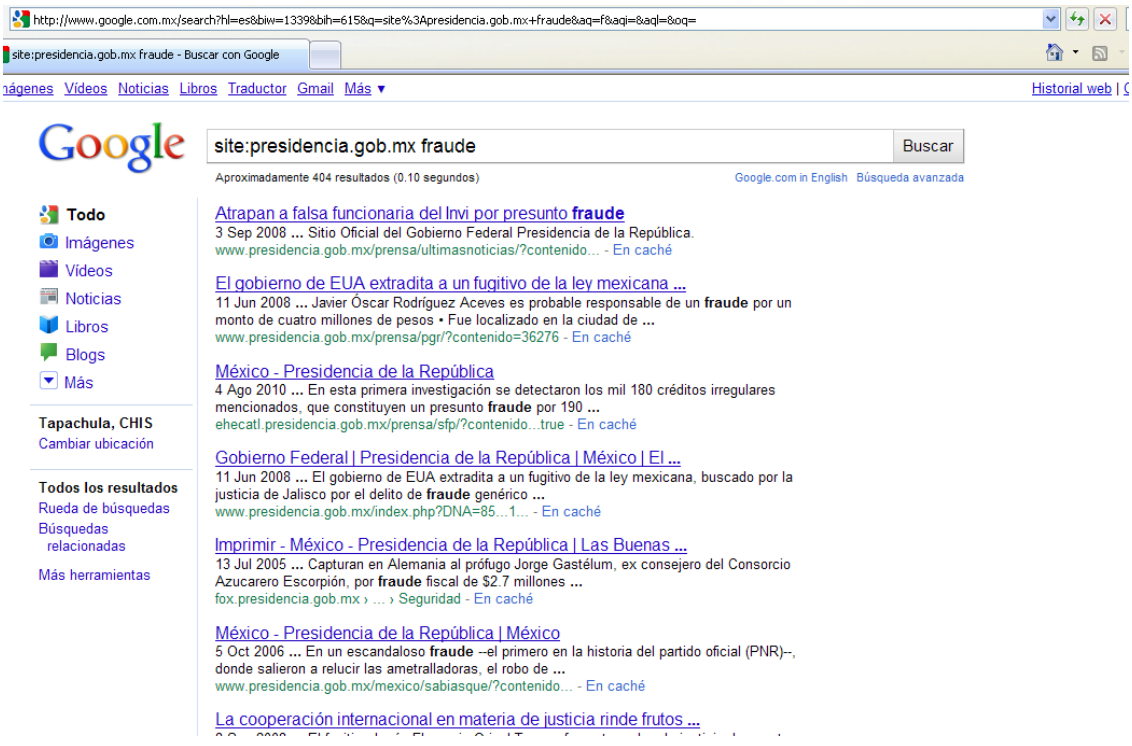
allfiletype	all filetype:xls empleados site:gob.mx	Esto buscara un fichero con números telefónicos también en sitios del gobierno mexicano.



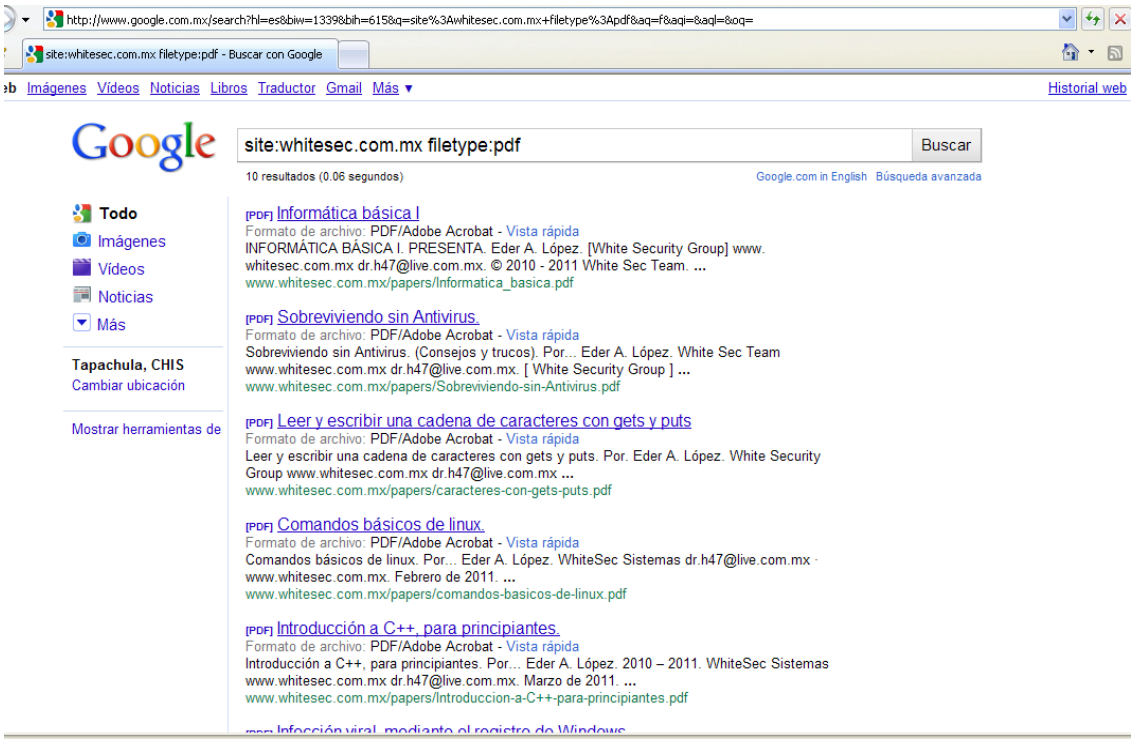
allinurl	all inurl:login.asp intitle:intranet site:com	Esto buscara ficheros login.asp de acceso a intranets.



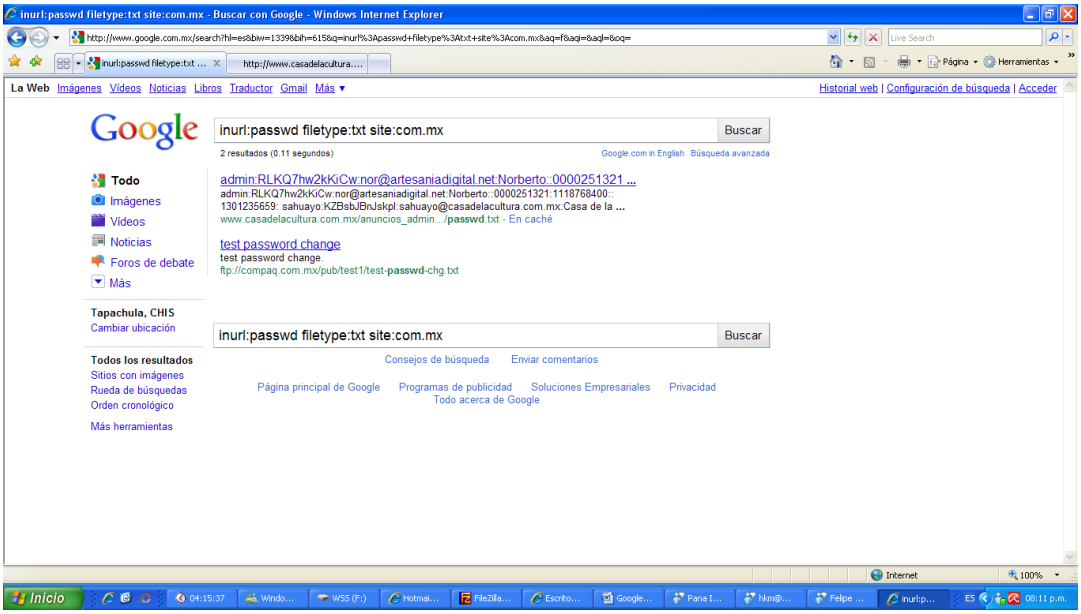
site	site:presidencia.gob.mx fraude	Buscara todo lo que tenga que ver con fraudes alojado en presidencia.gob.mx



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



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
- 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
- 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 articulo 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

---

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

Dr. H47
WhiteSec Sistemas.

www.whitesec.com.mx
dr.h47@live.com.mx
Abril 21 de 2011.

###

TH3 3ND