GOOGLE HACKING

Google Hacking es una técnica en informática que utiliza operadores para filtrar información en el buscador de Google. Además podemos encontrar otras aplicaciones de agujeros de seguridad en la configuración y el código informático que se utilizan en las páginas web.

Hay cientos de publicaciones en la red sobre este tema, pero al igual he visto, 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. Quiero observar que “saber utilizar los parámetros avanzados de búsquedas de google, no nos convierte en pentesters, analistas y mucho menos en hackers”.

Que puedo encontrar a través de Google Hacking?

Las técnicas que búsqueda a través del buscador de google, nos permiten 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 más 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.

PARAMETRO	MODO DE EJECUCIÓN	DETALLES
Inurl	inurl:login.asp	Busca el sitio que tengan “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.Esto dependerá enteramente 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, Cédulas de identidad, 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: lnxnetwork.com	Este operador muestra todos los sitios web que en sus paginas tengan links que apunten hacia el sitio web www.lnxnetwork.com, 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.
Autor	autor: José Hernandez	Esto hará una búsqueda en google por todos sitios, foros, blogs, en la cual haya comentado e iniciado un tema la persona en cuestión: José Hernandez.

Site	site:lnxnetwork.com 'hacking'	Esto buscara dentro de lnxnetwork.com y mostrara todos los enlaces donde encuentre la palabra “hacking”. OBS.: 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.
allinurl	inurl:passwords.txt site:com	Esto buscara el fichero passwords.txt dentro de todos los sitios .com que logre escanear.
allfiletype	filetype:xls cedula site:mec.gov.py	Esto buscara un fichero con datos de cedulas en sitios del gobierno.
allinurl	all inurl:login.asp intitle:intranet site:com all inurl:login.php intitle:intranet site:com	Esto buscara ficheros login.asp de acceso a intranets que estén expuestas en Internet.
Site	site:presidencia.gov.py fraude	Buscara todo lo que tenga que ver con fraudes alojado en el sitio presidencia.gov.py
	site:presidencia.gov.py nomina	Buscara todo lo que tenga que ver con la nómina de funcionarios alojado en el sitio presidencia.gov.py
Site	site:gov.py filetype:pdf	Buscara en todos los sitios “.gov.py” todos los ficheros .pdf alojados en los servidores.
Site	site:com inurl:passwd filetype:log	Esto buscara dentro de los sitios .com en el directorio passwd el log de contraseñas.
Inurl	filetype	También se puede usar así: inurl:passwd filetype:txt site:com
Inurl	inurl:pass filetype:sql site:com	Esta búsqueda le permitirá accede a archives SQL que contengan password
Inurl	inurl:users filetype:sql site:com	Esta búsqueda le permitirá accede a archives SQL que contengan usuarios
Filetype	filetype:xls password site:.mil	Buscaría archivos con extensión exel en los sitios militares, que contengan la palabra password
Site	site:static.ow.ly/docs/ intext:@gmail.com | Password	Busca en el sitio static.ow.ly archivos con contraseñas de usuarios para realiza el login en static.ow.ly

Inurl	inurl:DiGIR.php	Búsqueda de archivos interesantes (juicy)
Filetype	filetype:sql intext:wp_users phpmyadmin	Búsqueda del usuario administrador del wordpress en tablas SQL.
Genérica	"Index of /wp-content/uploads/backupbuddy_backups" zip	Realiza una búqueda generica de backup de bases de datos de wordpress
Inurl	inurl:top.htm inurl:currenttime	Realiza una búsqueda de sitios que tengas dispositivos conectados a Internet (cámaras, impresoras, etc).
Intext	intext:"Hello visitor from" ext:asp	Busca reslpaldos sobre
Algunas que otras contraseñas: allinurl:auth_user_file.txt intitle:"Index of" config.php intitle:index.of.etc filetype:xls username password email		
intitle	intitle:"Index of" ".htpasswd" "htgroup" -intitle:"dist" -apache -htpasswd.c	Busca archives de configuración apache web server que pudieran contener contraseñas.
intitle	intitle:"Index of" .mysql_history	Busqueda de archives relacionados a mysql


LNXnetwork
SOLUCIONES ALTERNATIVAS


Centro de Ethical Hacking & Security