Google Hacking

Banyak sekali website yang berguguran dengan memanfaatkan pencarian pada Google untuk menemukan targetnya. Seperti Worm Santy yang melakukan defacing secara massal dengan memanfaatkan Google. Dalam hitungan hari ribuan website tampilan utamanya berubah. Tulisan ini dibuat untuk memahami bagaimana melakukan pencarian yang baik dengan menggunakan Google. Pada bagian akhir juga terdapat trik-trik dan keyword yang sering digunakan untuk melakukan pencarian file dan juga bagaimana mencari target dengan memanfaatkan Google.

Penggunaan Dasar

Google tidak “case sensitive”.
Keyword: linux = LINUX = LiNuX
Akan menghasilkan hal yang sama

2. AND
Secara Default Google menggunakan keyword and.
Keyword: menjadi hacker
Hasilnya pencarian akan mengandung kata “menjadi” dan “hacker”

OR
Digunakan untuk menemukan halaman yang setidaknya berisi salah satu dari keyword. Note: OR dituliskan dengan huruf besar semua.
Keyword: hacker OR cracker
Hasilnya pencarian akan mengandung kata “hacker” atau “cracker”

+
Google akan mengabaikan pencarian dengan kata-kata umum seperti “how” dan “where”. Jika kata-kata umum ini begitu penting, anda bisa menambahkan “+” didepan keyword tersebut.
Keyword: hacker how ==> Kata “how” akan diabaikan
Keyword: hacker +how ==> Kata “how” akan diikutsertakan

–
Tanda minus “-” bisa digunakan untuk mengecualikan kata-kata tertentu dalam pencarian. Misal kita ingin mencari kata “linus tanpa linux”, kita bisa menggunakan “linus -linux”

*
Google tidak mendukung pencarian * sebagai pengganti huruf.
Misalkan kita ingin mencari dengan kata depan menja*
Google tidak mencari kata “menjamu”, “menjadi”, “menjalar”, dll
Google akan menghasilkan pencarian hanya yang mengandung kata “menja”.
Tetapi google mendukung penggunaan * dalam pencarian kalimat.
Keyword: “menjadi * hacker”

Hasilnya pencarian dapat menghasilkan “menjadi seorang hacker”, “menjadi white hacker”, dll.

“”
Dapat digunakan untuk mencari kata yg lengkap.
Keyword: “menjadi hacker”
Hasilnya pencarian akan mengandung kata “menjadi hacker”

8. ?
Dapat digunakan untuk mencari pada direktori Google
Keyword: ?intitle:index.of? mp3
Hasilnya pencarian akan Mp3

OPERATOR SPESIAL

1. intitle: Untuk mencari kata-kata dari judul suatu halaman web.
Keyword: intitle:Admin Administrasi
Keyword tersebut akan mencari judul halaman “Admin” dengan deskripsi “Administrasi”

2. allintitle: Untuk mencari kata-kata dari judul halaman web secara lengkap.
Keyword: allintitle:Admin Administrasi
Keyword tersebut akan mencari judul halaman yang mengandung kata “Admin” dan “Administrasi”

3. inurl: Digunakan untuk mencari semua URL yang berisi kata-kata tertentu.
Keyword: inurl:Admin Administrasi
Keyword tersebut akan mencari URL yang mengandung kata “Admin” dengan deskripsi “Administrasi”

4. allinurl: Digunakan untuk mencari semua URL yang berisi kata-kata tertentu.
Keyword: allinurl:Admin Administrasi
Keyword tersebut akan mencari URL yang mengandung kata “Admin” dan “Administrasi”

5. Site: Untuk mencari dalam suatu situs tertentu saja
Keyword: site:echo.or.id
Semua pencarian hanya berdasarkan site “echo.or.id”

6. cache: Ketika Googlebot mengindeks suatu situs, google akan mengambil snapshot dari semua halaman yang telah terindeks. Operator ini membantu melihat halaman-halaman yang telah dicache.
Keyword: cache:echo.or.id

Misalkan site aslinya sudah tidak aktif, anda tetap dapat melihatnya pada snapshot/cache yang disimpan oleh Google.

7. Define: Operator ini digunakan untuk mencari definisi dari frasa tertentu. Semua kata yang diketik setelah operator ini akan diperlakukan sebagai satu frasa.
Keyword: define:hacker

8. Filetype: Jika kita mencari jenis file tertentu yang berisi informasi yang anda inginkan kita bisa menggunakan operator ini.
Keyword: “hacker” filetype:pdf
Adobe Portable Document Format (pdf)
Adobe PostScript (ps)
Lotus 1-2-3 (wk1, wk2, wk3, wk4, wk5, wki, wks, wku)
Lotus WordPro (lwp)
MacWrite (mw)
Microsoft Excel (xls)
Microsoft PowerPoint (ppt)
Microsoft Word (doc)
Microsoft Works (wks, wps, wdb)
Microsoft Write (wri)
Rich Text Format (rtf)
Shockwave Flash (swf)
Text (ans, txt)

- link: Untuk mencari tahu berapa banyak link ke suatu situs, kita bisa menggunakan operator link.
Keyword: link:www.google.com

- related: Untuk mencari halaman yang isinya mirip dengan URL tertentu.
Keyword: related:www.google.com

Manipulasi URL Google

1. Interface google

And bisa mengganti interface google dengan mengganti variabel hl
(default google hl=en => bahasa inggris)
Misalkan kita mengubah interface-nya menjadi bahasa Indonesia.
Ex:
http://www.google.com/search?hl=en&lr=&q=site%3Aecho.or.id&btnG=Search
Hasil modifikasi URL
http://www.google.com/search?hl=id&lr=&q=site%3Aecho.or.id&btnG=Search

2. Bahasa Tertentu
Anda dapat mengganti hasil pencarian hanya pada bahasa tertentu. Hal ini dilakukan

dengan modifikasi variabel lr. (default google lr=lang_en => bahasa inggris)
Misalkan kita hasil pencarian hanya bahasa Indonesia.
Ex:
http://www.google.com/search?hl=en&lr=&q=site%3Aecho.or.id&btnG=Search
Hasil modifikasi URL
http://www.google.com/search?hl=en&lr=lang_id&q=site%3Aecho.or.id&btnG=Search

Menampilkan Site Perhalaman

Secara default google akan menampilkan 10 site perhalaman. Anda dapat mengubahnya secara langsung melalui URL-nya, dengan menambahkan variable num pada URL
Penggunaan num antara 1-100
Ex:
http://www.google.com/search?hl=en&lr=&q=site%3Aecho.or.id&btnG=Search
Hasil modifikasi URL
http://www.google.com/search?num=100&hl=en&lr=&q=site%3Aecho.or.id&btnG=Sea
rch

Menentukan Hasil Berdasarkan Bulan

as_qdr=mx: merupakan variabel lainnya yang dapat digunakan. Variabel ini digunakan menentukan hasil berdasarkan bulan. x antara 1-12
Ex:
http://www.google.com/search?hl=en&lr=&q=site%3Aecho.or.id&btnG=Search
Hasil modifikasi URL
http://www.google.com/search?hl=en&lr=&as_qdr=m1&q=site%3Aecho.or.id&btnG=Se
arch

5. Safe=off: arti dari variabel ini filter “SafeSearch” dimatikan. “SafeSearch” untuk memfilter hasil pencarian sexual.

Dengan pengetahuan di atas anda dapat membuat sendiri form Google di computer sendiri. Sehingga tidak perlu lagi mengunjungi http://www.google.com terlebih dahulu (kecuali anda menggunakan brwoser yang support google secara built-in atau menggunakan Google Toolbar). Dengan melakukan ini kita bisa menghemat bandwidth ke luar negeri Karena bandwidth di Indonesia mahal ……..

Contoh script google.html lengkap dengan varabielnya.

Bof Google.Html

<form action=”http://www.google.com/search” name=f>
Variabel num: <input name=num value=10>
Variabel hl: <input name=hl value=en>
Variabel lr: <input name=lr value=lang_id>
Variabel as_qdr: <input name=as_qdr value=m12>

Variabel safe: <input name=safe value=off>
<input maxLength=256 size=55 name=q value="">
<input type=submit value="Google Search" name=btnG>
</form>

Eof Google.Html

Anda tinggal menghilangkan Variabel yang tidak anda inginkan atau menambahkan apapun disana. Semuanya terserah kepada anda Berikut merupakan script default pencarian google.

Bof Google.Html

<form action="http://www.google.com/search" name=f>
<input maxLength=256 size=55 name=q value="">
<input type=submit value="Google Search" name=btnG>
</form>

EOF google.html

Google masih terus dikembangkan. Untuk melihat apa yang sedang dikembangkan Google. Anda bisa ke http://labs.google.com

Tips & Tricks

Dari dasar-dasar dan spesial operator tersebut anda bisa mencampurkan operator-operator tersebut.
Ex:
Keyword: site:echo.or.id, menghasilkan semua site echo.or.id. Kemudian anda bisa mencoba keyword: site:echo.or.id hacker, akan menghasilkan semua site echo.or.id yang mengandung kata hacker.

Kita juga dapat melakukan pencarian secara spesifik melalui google.
Untuk melakukannya anda dapat ke site berikut:
- http://www.google.com/bsd
- http://www.google.com/mac
- http://www.google.com/linux
- http://www.google.com/microsoft
- http://www.google.com/univ/education

Berbagai trik keyword pada Google:
parent directory books -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
parent directory /appz/ -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
parent directory DVDRip -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
parent directory video -xxx -html -htm -php -shtml -opendivx -md5 -md5sums

parent directory Gamez -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
parent directory MP3 -xxx -html -htm -php -shtml -opendivx -md5 -md5sums

intitle:index of intitle:mp3 -html -htm name size
intitle:index of intitle:video -html -htm name size
intitle:index of intitle:cgi-bin passwd -html -htm name size
intitle:index of intitle:cgi-bin password -html -htm name size

inurl:”admin.mdb” -html
inurl:”password.mdb” -html
inurl:”data.mdb” -html
“phpMyAdmin” “running on” inurl:”main.php”
intitle:”PHP Shell” “Enable stderr” php