HACKING

Disampaikan pada Workshop Basic Hacking di STIKI pada tanggal 24 & 25 Februari 2007,
Diadaptasi dari buku Google Hacking karangan Efvy Zam Kerinci.

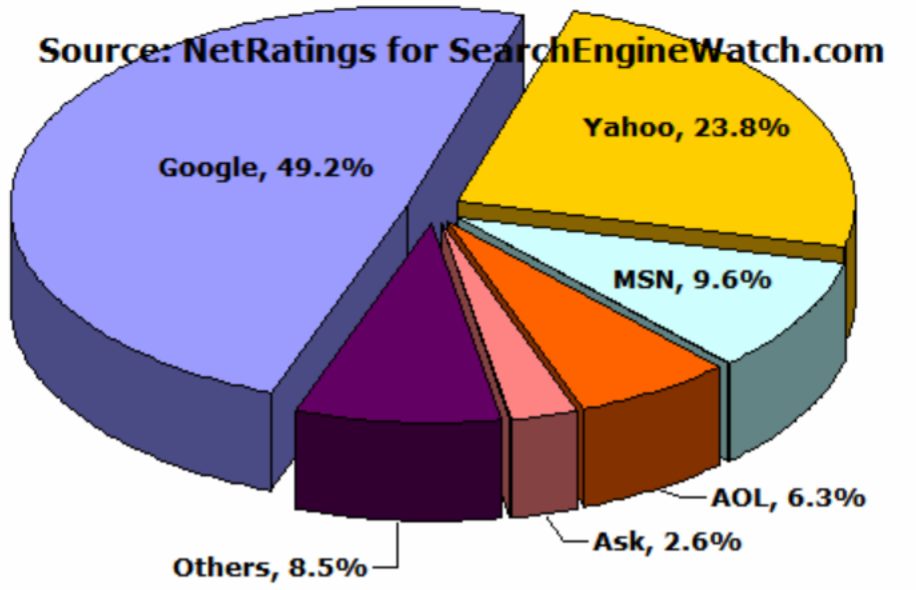
•

A. Ismail Marjuki
admin@stiki.ac.id

•

Sekilas Tentang Google

Google adalah salah satu mesih pencari yang terpopuler di dunia saat ini. Kepopuleran Google dapat kita lihat pada situs www.searchenginewatch.com. Lihat statistik di bawah ini:



Pengertian Google Hacking

Yang dimaksud dengan Google Hacking disini menurut Efvy Zam Kerinci adalah melakukan aktifitas hacking menggunakan Google sebagai sarananya. Sehingga Anda gak boleh salah faham mengartikan kita akan meng-hack situs Google yaa…

Dalam workshop Google Hacking kali ini, kita akan mencoba mendapatkan informasi-informasi berharga mengenai target hacking kita menggunakan search engine Google. Informasi tersebut meliputi:

- Target menjalankan Sistem Informasi apa?
- Target menggunakan web server apa?
- Apa saja kelemahan (vulnerabilities) pada target?
- Data sensitif apa yang terdapat dalam file dan direktori publik milik target?
- Bagaimana cara menampilkan file/data pada target yang tidak bisa dimunculkan dengan cara biasa?

Oke, beberapa dari pertanyaan di atas akan kita jawab menggunakan mesin pencari Google dalam kurun waktu satu jam ke depan. Tentu saja untuk itu kita paling tidak harus menguasai teknik pencarian yang paling dasar menggunakan Google.

Yang Perlu Anda Tahu

Sebelum kita melangkah lebih jauh, Anda perlu memahami operator apa saja yang dapat digunakan untuk Google, operator-operator ini nantinya dapat mempersempit pencarian dan penggunaan operator yang tepat akan dapat memperoleh hasil yang maksimal.

Berikut ini beberapa operator dasar dan logika boolean yang dapat diterapkan pada Google:

1. AND atau Tanda Tambah (+)

Contoh penggunaan:

Akan menghasilkan pencarian yang mengandung kedua kata tersebut. Secara default, Google menggunakan logika AND, sehingga Anda tidak perlu menuliskannya.

Hasilnya:

2. OR

Logika OR digunakan untuk mencari halaman web yang paling tidak mengandung salah satu unsur dari kata-kata yang dimasukkan.

Contoh penggunaan:

Hasil:

3. Tanda Minus

Contoh penggunaan:

Akan menampilkan halaman web yang mengandung kata Hacker, tapi tidak mengandung kata Cracker. Operator ini **tidak** akan menampilkan kata yang mengandung tanda minus.

4. Tanda Asterik (*)

Tanda asterik pada pencarian ini bisa berarti 'apa saja'.

Contoh penggunaan:

Hasil: akan menampilkan kata-kata antara "STIKi" dan "Informatika".

Hasil: hasil yang didapatkan adalah kata lain setelah "how to hack"

5. Tanda Kutip (" ")

Digunakan untuk mencari teks yang diapit oleh tanda kutip tersebut tanpa ada pemisahan kata.

Contoh penggunaan:

Hasilnya akan menampilkan halaman web yang mengandung kata STIKI Malang dalam satu rangkai.

Teknik Dasar Google Hacking

Oke, sebelum Anda mengantuk dan menganggap penjelasan saya bertele-tele, kita langsung saja memasuki inti acara kita pada hari ini. Yaitu menguasai teknik dasar dari Google Hacking.

Perhatikan anatomi dasar dari sebuah web browser Rubah Berapi berikut:

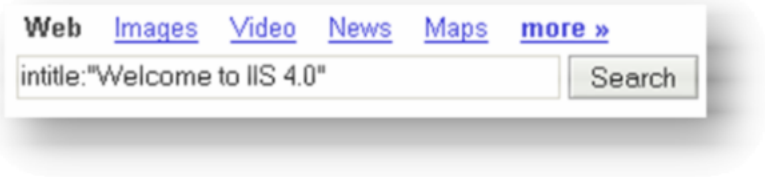
Ada beberapa sintaks dasar yang dapat Anda gunakan untuk proses Google Hacking , antara lain:

1. intitle:

Fungsi: untuk membatasi hasil pencarian hanya pada judul halaman atau title.

Yang bisa kita dapatkan: mengetahui ciri-ciri sebuah sistem server, misalnya server tersebut menggunakan web server apa? Dst.

Contoh penggunaan:



Dengan perintah di atas, kita dapat mengetahui server-server mana saja yang masih menggunakan halaman default (bawaan) dari web server IIS 4.0.

2. inurl:

Fungsi: untuk mencari hanya pada bagian URL saja, dengan mengacuhkan title dan lainnya.

Yang bisa kita dapatkan: sebagai satu contoh kita bisa mendapatkan database Access dari sebuah situs e-commerce yang bisa berisi informasi tentang pengguna e-commerce tersebut.

Contoh penggunaan:

3. site:

Fungsi: untuk membatasi pencarian query hanya pada situs atau domain tertentu.

Yang bisa kita dapatkan: informasi tentang sub domain dari sebuah situs, dll.

Contoh penggunaan:

4. filetype:

Fungsi: untuk mencari file dengan jenis tertentu.

Yang bisa kita dapatkan: beragam jenis password yang biasa disimpan oleh Administrator pada file berjenis xls atau txt.

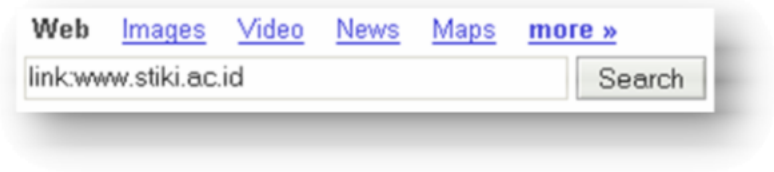
Contoh penggunaan:

5. link:

Fungsi: untuk menampilkan daftar situs yang memiliki link pada situs tertentu.

Yang bisa kita dapatkan: mengetahui berapa banyak link yang menuju pada suatu situs.

Contoh penggunaan:



6. related:

Fungsi: untuk menampilkan daftar situs yang mungkin mirip atau serupa dengan situs yang dicari.

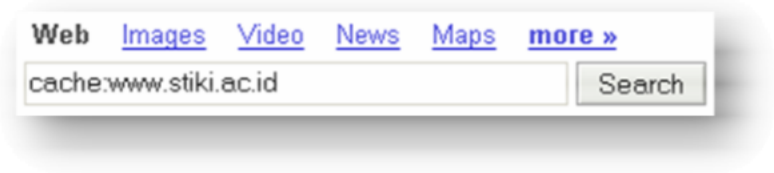
Contoh penggunaan:

7.cache:

Fungsi: untuk menampilkan rekaman tampilan suatu situs yang tersimpan pada database google.

Yang bisa kita dapatkan: snapshot suatu situs yang mungkin sudah tidak online lagi.

Contoh penggunaan:



8.intext:

Fungsi: mencari kata-kata pada body situs tertentu.

Yang bisa kita dapatkan: form administrator login, dll.

Contoh penggunaan:

9.define:

Fungsi: menampilkan pengertian dari sebuah kata yang dicari.

Contoh penggunaan:

Hasilnya adalah pengertian cracker dari beberapa situs di Internet.

10. **info**

    Fungsi:

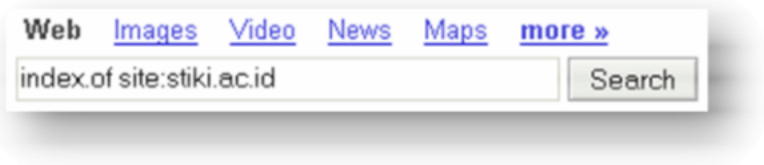
    Yang bisa kita dapatkan:

    Contoh penggunaan:

Yoek, kita mulai hacking-nya…

Sekali lagi sebelum Anda semua bosan mbaca modul ini, dan tertidur… saya langsung mulai saja proses hacking-nya.

1. **Melihat-lihat Direktori Sensitif orang lain:**



Dengan perintah di atas, banyak informasi yang bisa kita dapatkan dari domain stiki.ac.id. Informasi tersebut adalah berupa isi direktori web server yang memiliki direktori index yang dapat diakses.

Index of ini juga dapat digunakan untuk memperoleh informasi-informasi sensitif seperti password dan lainnya yang tidak bisa diakses dengan cara pencarian biasa. Hal ini dimungkinkan karena adanya kesalahan konfigurasi dari web server yang bersangkutan.

Tabel di bawah ini adalah perintah-perintah lain yang dapat kita gunakan untuk mengeksplorasi informasi-informasi penting melalui Google:

Google Search	Keterangan
intitle:index.of.config	**Direktori config berisi tentang konfigurasi web server yang seharusnya tidak dapat dilihat oleh umum karena terdiri dari beberapa file yang bisa dilihat sedangkan beberapa file lain merupakan file yang terenkripsi. Informasi lainnya yang bisa didapatkan adalah bermacam-macam ports, hak akses keamanan, dsb.**
"Welcome to the directory listing of" "NetworkActiv-Web-Server"	**Sintaks ini digunakan untuk melihat isi direktori dari NetworkActiv-Web-Server.**
"Directory Listing for" "Hosted by Xerver"	**Menampilkan daftar direktori dari web server Xerver.**
intitle:"Folder Listing" "Folder Listing" Name Size Date/Time File Folder	**Menampilkan daftar direktori dari web server Fastream NETFile.**
filetype:ini Desktop.ini intext:mydocs.dll	**Untuk menemukan berbagai folder yang di-sharing dalam MyDocument.**

2. **Mencari Kelemahan suatu Situs:**

Untuk mengetahui kelemahan atau vulnerable suatu situs, kita perlu memperdalam tentang penggunaan sintaks inurl dan allinurl.

Contoh penggunaan:

Tujuannya adalah untuk menampilkan semua link yang memberikan akses pada direktori system32. sebab direktori system32 ini merupakan salah satu direktori terlarang. Jadi, apabila Anda dapat melihat isi server bahkanmengendalikkannya melalui web. Apalagi, jika Anda beruntung dan bisa mengakses file cmd.exe dalam direktori system32 tersebut. Anda bisa mengambil alih sistem dan melakukan berbagai kegiatan hacking.

Pada situs yang saya coba, saya bahkan dapat mengambil alih komputer korban, dengan menjalankan perintah cmd.exe, berikut capture-nya:

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Date: Wed, 19 Sep 2001 22:14:56 GMT
Content-Type: application/octet-stream
Volume in drive C has no label.
Volume Serial Number is 6878-FC6E

 Directory of C:\InetPub\scripts

09/19/01  04:57p        <DIR>          .
09/19/01  04:57p        <DIR>          ..
08/01/01  11:10a        <DIR>          iisadmin
02/10/00  10:00a                15,760 nsiislog.dll
11/18/99  02:04p               208,144 root.exe
06/22/01  06:58a        <DIR>          samples
06/22/01  06:58a        <DIR>          tools
               7 File(s)        223,904 bytes
                           1,400,608,256 bytes free
```

Berikut ini sintaks lain yang mungkin dapat Anda coba sendiri:

Google Search	Keterangan
intitle:"MvBlog powered"	**MvBlog adalah sebuah aplikasi pembangun blog yang memiliki kelemahan antara lain pada validasi multiple-input, html injection, sql injection. Jika exploit terhadap aplikasi ini berhasil, memungkinkan untuk mengakses atau mengubah data.**
intitle:"XOOPS Custom Installation"	**XOPPS adalah sebuah CMS seperti Joomla. Pada menu cepat installasinya, memungkinkan user untuk memodifikasi beberapa parameter installasi, seperti username, password, dan tabel installasi.**
inurl:rpSys.html	**Halaman konfigurasi berbasis web untuk beberapa jenis sistem. Dan kebanyakan dari sistem ini tidak ber-password.**
intitle:"Uploader - Uploader v6" - pixloads.com	**File upload Server, sangat berbahaya jika dipasangkan dengan mytrashmail.com**
"you can now password" | "this is a special page only seen by you. your profile visitors" inurl:imchaos	**Mencari halaman penelusuran link dari Imchaos, disini kita bisa mendapatkan AIM, IP Address dan info lainnya. Juga dapat melihat dan menghapus halaman yang ada.**

Daftar Pustaka

Buku Google Hacking, Evry Zam Kerinci

http://johnny.ihackstuff.com

http://johnny.ihackstuff.com/forums/