Agenda

Introduction
The Basic
Google Hacking Techniques
How to Protect your Websites
Introduction

• First step in attacking websites or penetration testing is reconnaissance

• Google is an ideal tool for this

• If done carefully, targets won’t event notice they were being profiled and examined on their weak points.
The Basics

• To set the stage for what I will demo, it is necessary to understand some of Google’s advanced search functions.
• This will not be an exhaustive list, just an intro.
• Creative use of these functions is the key to successful Google Hacking.
The Basics

We all know basically how to use Google. But how many of us use their Preferences link?
The Basics

Now let's take a look at Advanced Search.
Let's try looking for PDF files within progressive.com.
The Basics

Now its time to take a close look on the interesting Google Search Commands
DefconPH.org - Index
Welcome, Guest. Please login or register. 1 Hour, 1 Day, 1 Week, 1 Month, Forever. Login with username, password and session length ...

Close window Having problems hearing this? Try a direct link to it.

http://defconph.org/forum/index.php?action=verificationcode;rand=aaafe5039eeec452486d3308c9c5cb36.format=.wav;format=.wav ...
defconph.org/forum/index.php?PHPSESSID=dfaad0ef5ef7d95385b265a06c2921fc&action=ver... - 2k - Cached - Similar pages -

Close window Having problems hearing this? Try a direct link to it.

http://defconph.org/forum/index.php?action=verificationcode;rand=b05dfbc7be224fdaa5cb9b11779fcbfd.format=.wav;format=.wav ...
defconph.org/forum/index.php?PHPSESSID=851bc448e6d7924a5e489b06f15e4723&act... - 2k - Cached - Similar pages -

Print Page - funnies section
post any funny comic strips, pictures, images, quotes, etc. here that caters to our 31337 sense of humors :D I'll start with an sql-inject comic strip (see ...
In order to show you the most relevant results, we have omitted some entries very similar to the 3 already displayed.
If you like, you can repeat the search with the omitted results included.
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.5 (GNU/Linux)

mQGiBEj96YRBADkM7X15GxJzDHQEhylKoj8fWhHSuMYeWWX+yaUjZX6x33Cek4F...

www.defconph.org/pgp/semprix.key - 3k - Cached - Similar pages -

-----END PGP PUBLIC KEY BLOCK-----
The Basics

There are many more advanced operators

Some other things to keep in mind
- Google queries are not case sensitive.
- The * wildcard represents any word
  - Example: “* hacker quote”
- Google stems words automatically
  - Example: “hacker blog quote” brings up sites with “hacker … “.
The Basics

- The + symbol forces inclusion of a certain word.
  - “blog defconph +defconph”
- We’ve already seen the – symbol.
- The | symbol provides boolean OR logic.
  - “blog defconph +inurl:(defconph | maxtor)”
This is getting boring already, let's get this stuff out of the way and get some Google Hacking.
DefconPH Beer Talk 1
@ Handuraw, 460 Gorordo Avenue, Cebu City
December 20, 2008 1pm - 6pm
We used Fiddler to Debug our session
We will check if Google cache allows us to become anonymous.
Opplssss, we are still hitting directly to the site.
<table>
<thead>
<tr>
<th>#</th>
<th>Result</th>
<th>Protocol</th>
<th>Host</th>
<th>URL</th>
<th>Body</th>
<th>Cache Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>200</td>
<td>HTTP</td>
<td><a href="http://www.fiddler2.com">www.fiddler2.com</a></td>
<td>/fiddler2/updatecheck.asp...</td>
<td>520</td>
<td>private</td>
</tr>
<tr>
<td>1</td>
<td>200</td>
<td>HTTP</td>
<td>72.14.235.132</td>
<td>/search?q=cache:jo6xhV/...</td>
<td>1,887</td>
<td>private</td>
</tr>
<tr>
<td>2</td>
<td>502</td>
<td>HTTP</td>
<td>bdc-iss005.na.pg.com</td>
<td>/</td>
<td>512</td>
<td></td>
</tr>
</tbody>
</table>
Trolling Emails on Google
Network Mapping

- A hacker could use Google to obtain a list of all defconph.org domain names that are indexed by Google.
- Some interesting domain names may be found deep within the search results.
Automated Google Hacking

• It would be easy write a script that automates these types of queries against google.com and compiles the results.

• Lots of sample code is available, including C# code.

• A tool called GooScan does this.

• But this goes against Google’s Terms of Use.

• Google is rumored to keep a “black list” of bad IP addresses, so be careful!
Google Query APIs

- Google used to provide a web service API for doing automated queries.
- This API is no longer available.
- Alternatives that break Google’s Terms of Use:
  - Evil API
  - Aura API
DNS–Mine.pl

- Attempts to get a list of domain names, similar to what I just demonstrated manually.
- Written by Roelof Temmingh of Sensepost.com
- Uses Google API
Sitedigger

- Automated Google hacking tool from Foundstone
- Uses Google API
- Written in .Net
- Uses Google Hacking Database
Google Hacking Database

- Located at johnny.ihackstuff.com
- Contains list of Google hacks, constantly updated
- Demo
How To Protect Your Websites From Google Hackers

- In general, be very careful about what content you place on your Internet-facing websites.
- Do not display detailed error messages.
- Do not allow directory browsing.
How To Protect Your Websites From Google Hackers

- Keep all of your links environment specific
- Keep your name and email out of HTML comments and don’t post on Google Groups with your work email account.
- Configure your web server to only serve up a list of “safe” file types and to respond with “File Not Found” for any unsafe types.
For More Info

- “Google Hacking For Penetration Testers” Volume 2 by Johnny Long
- http://johnny.ihackstuff.com
- http://www.sensepost.com
- http://www.foundstone.com
- http://www.google.com
QUESTIONS ?????????????????????