Johnny Long
CSC

Google Hacking for Penetration Testers

Google Hacking returns for more guaranteed fun this year at Blackhat USA! If you haven’t caught one of Johnny’s Google talks, you definitely should. Come and witness all the new and amazing things that can be done with Google. All new for BH USA 2005, Johnny reveals basic and advanced search techniques, basic and advanced hacking techniques, multi-engine attack query morphing, and zero-packet target footprint printing and recon techniques. Check out Google’s search-blocking tactics (and see them bypassed), and learn all about using Google to locate targets Google doesn’t even know about! But wait, there’s more! Act now and Johnny will throw in the all new “Google Hacking Victim Showcase, 2005” loaded with tons of screenshots (and supporting queries) of some of the most unfortunate victims of this fun, addictive and deadly form of Internet nastiness. Think you’re too über to be caught in a Google talk? Fine. Prove your badness. Win the respect of the audience by crushing the live Google Hacking contest! Submit your unique winning query by the end of the talk to win free books from Syngress Publishing and other cool gear! Or don’t. Just listen to your friends rave about it. Whatever.

Johnny Long is a “clean-living” family guy who just so happens to like hacking stuff. Over the past two years, Johnny’s most visible focus has been on this Google hacking “thing” which has served as yet another diversion to a serious (and bill-paying) job as a professional hacker and security researcher for Computer Sciences Corporation. In his spare time, Johnny enjoys making random pirate noises (“Yarrr!”), spending time with his wife and kids, convincing others that acting like a kid is part of his job as a parent, feigning artistic ability with programs like Bryce and Photoshop, pushing all the pretty shiny buttons on them new-fangled Mac computers, and making much-too-serious security types either look at him funny or start laughing uncontrollably. Johnny has written or contributed to several books, including “Google Hacking for Penetration Testers” from Syngress Publishing, which has secured rave reviews and has lots of pictures.
Google Hacking for Penetration Testers

Using Google as a Security Testing Tool
Johnny Long
Johnny@hakintosh.com

Sample Slides. Show up for all new Blackhat Goodness!

What we're doing

• We're covering many techniques covered in the 'Google Hacking' book.
• But since this is Blackhat, we'll go deeper!
• For much more detail, I encourage you to check out "Google Hacking for Penetration Testers" by Syngress Publishing.

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense
Advanced Operators

Before we can walk, we must run, in Google’s terms this means understanding advanced operators.

Sample Slides. Show up for all new Blackhat Goodness!

Advanced Operators

- Google advanced operators help refine searches.
- They are included as part of a standard Google query.
- Advanced operators use a syntax such as the following:

```
operator: search_term
```

- There’s no space between the operator, the colon, and the search term!

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense
Advanced Operators at a Glance

- Some operators can only be used to search specific areas of Google, as these columns show.

Crash course in advanced operators

- Site can search for site:
- Inurl can search for query in URL:
- Filetype can only search file types, which may be used to debug attacks.

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense
Advanced Google Searching

There are many ways to find the same page. These individual queries could all be fed to find the same page.

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense
Google Hacking Basics

Pertaining operators together in intelligent ways can cause seemingly innocuous query...

osCommerce
om/catalog/admin/orders.php+files

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense
Google Hacking Basics

Let’s take a look at some basic techniques:

Anonymous Googling
Special Characters

Sample Slides. Show up for all new Blackhat Goodness!

Anonymous Googling

The cache link is a great way to get
content without its
displayed from the site.
The question is, where
exactlly does that
content come from?
Anonymous Googling

- Some folks use the cache link as an anonymizer, thinking the content comes from Google. Let's take a closer look.

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense
Anonymous Googling

- Obviously we touched the site, but why?
- Here's more detailed toplump output

Sample Slides. Show up for all-new Blackhat Goodness!

digital self defense
Anonymous Googling

This time, the entire conversation was between a user (192.168.2.232) and Google (23.233.167.104)

Sample Slides: Show up for all new Blackhat Goodness!

Anonymous Googling

- What made the difference? Let's compare the two URLs:

  - Original:
    
    http://Example.com/Example.html
    
  - Cached Text Only:
    
    http://Example.com/Example.html

Sample Slides: Show up for all new Blackhat Goodness!
Anonymous Googling

- Anonymous Googling can be helpful, especially if combined with a proxy. Here's a summary.

Special Search Characters

- We'll use some special characters in our examples. These characters have special meaning to Google.
- Always use these characters without surrounding spaces!
  - (+) force inclusion of some things common
  - (-) exclude a search term
  - (*) use quotes around search phrases
  - (:) a single-character wildcard
  - (") any word
  - (:) boolean "OR"
  - Parentheses group queries ("waste is art" OR "waste is not art")
Introducing the GoogleDork Detection System! (GDDS)

- Google has started blocking queries, most likely as a result of worms that spam Google with "evil queries."

Sample Slides. Show up for all new Blackhat Goodness!

Bypassing GDDS Round 1: Case Modification

- Our original query looks like this:

http://www.google.com/search?hl=en&q=weed+man+machine+on+china+0+beach

- Shipped down, the query looks like this:

http://www.google.com/search?hl=en&q=weed%20man%20machine%20on%20china%200%20beach

- We can modify our query (make something.php is bad) by changing the case of the file extension, like so:

http://www.google.com/search?hl=en&q=weed%20man%20machine%20on%20china%200%20beach%20something.php

Sample Slides. Show up for all new Blackhat Goodness!

This works in the web interface as well.

digital self defense
Sample Slides. Show up for all new Blackhat Goodness!
Bypassing GDS: Why, Johnny?

- Q: Why show this, Johnny?
- A: Well, the bad guys are already doing it, that’s for sure.
- Never, ever assume that Google will protect you. Google’s blocks are generally put in place to stave off massive worm-style queries.
- If Google was able to effectively block all bad queries,
  - they could cut into the number of returned search results, hurting their market placement
  - They could show a willingness to compromise their product in the face of oppression, which sets a bad president.

Sample Slides. Show up for all-new Blackhat Goodness!

Pre-Assessment

There are many things to consider before building a database of which Google can help with. One thing example is the collection of email addresses and usernames.

Sample Slides. Show up for all-new Blackhat Goodness!

digital self defense
Trolling for Email Addresses

- A seemingly simple search uses the @ sign followed by the primary domain name.

Automated Trolling for Email Addresses

- We could use lynx to automate the download of the search results:

 lynx http://www.myEpsilon.com/show-email-lists

- We could then use regular expressions (like this puppy by Don Ranta) to troll through the results:

```regex
\b[A-Za-z0-9\-]+@\b[A-Za-z0-9\-]+\b
```

- Run through grep, this regexp would effectively find email addresses (including addresses containing IP numbers)

Sample Slides. Show up for all new Blackhat Goodness!
More Email Automation

- The `email miner` PERL script by Roelof Temmingh at sensepost will effectively do the same thing, but via the Google API.

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense
## More email address locations

<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>@</code> symbol</td>
<td>Look for email addresses at the end of the line.</td>
</tr>
<tr>
<td><code>mailto:</code></td>
<td>Look for <code>mailto:</code> links in HTML.</td>
</tr>
<tr>
<td><code>mailto:</code></td>
<td>Look for the <code>mailto:</code> tag in HTML.</td>
</tr>
<tr>
<td><code>@</code> symbol and <code>&gt;</code></td>
<td>Look for email addresses after the <code>&gt;</code> symbol.</td>
</tr>
<tr>
<td><code>mailto:</code> and <code>&gt;</code></td>
<td>Look for the <code>mailto:</code> tag after the <code>&gt;</code> symbol.</td>
</tr>
<tr>
<td><code>mailto:</code> and <code>@</code> symbol</td>
<td>Look for <code>mailto:</code> tags with <code>@</code> symbols.</td>
</tr>
<tr>
<td><code>mailto:</code> and <code>&gt;</code> symbol and <code>@</code> symbol</td>
<td>Look for <code>mailto:</code> tags with <code>&gt;</code> and <code>@</code> symbols.</td>
</tr>
</tbody>
</table>

Sample Slides. Show up for all new Blackhat Goodness!
Network Mapping

Google is an intuitions site tool for mapping out an Internet-related network. Let’s look at ways Google can help us discover targets and map out networks.

Basic Domain Crawling

*site:* operator narrows a search to a particular site, domain or subdomain.

One-page query lists every Google result from a web domain!

Sample Slides. Show up for all new Blackhat Goodness!
Basic Domain Crawling

As a security test, we need to get to the less obvious stuff.

www.microsoft.com is very obvious...

Basic Domain Filter

- To get rid of the more obvious crap, do a negative search.

Notice that the always "view" is missing, replaced by more interesting domains.

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense
Ugly Domain Filtering

- Repeating this process of site reduction, tracking what floats to the top leads to nasty big queries like:

... 

Sample Slides. Show up for all new Blackhat Goodness!

Ugly Domain Filter Gives Decent Results

- The results of such a big query reveal more interesting results...

... 

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense
**So what?**

- Well, honestly, host and domain enumeration isn't new, but we're doing this without sending any packets to the target we're analyzing.
- This has several benefits:
  - Low profile. The target can't see your activity.
  - Results are "ranked" by Google. This means that the most public stuff tends to the top. Some more "interesting stuff" trolls near the bottom.
  - "Hints" for follow-up research. You aren't just getting hosts and domain names, you get application information just by looking at the snippet returned from Google. One results page can be processed for many types of info. Email addresses, names, etc. More on this later on...
  - Since we're getting data from several sources, we can focus on non-obvious relationships. This is huge!
- Some downsides:
  - In some cases it may be faster and easier as a good guy to use traditional techniques and tools that connect to the target, but remember: the bad guys can still find and target you via Google!

Sample Slides. Show up for all new Blackhat Goodness!
Automated Crawling

- Google frowns on automation, unless you use tools written with their API. Know what you’re running unless you don’t care about their terms of service.
- We could easily modify our lynx retrieval command to pull more results, but in many cases, more results won’t equal more unique hosts.
- So, we could also use another technique to locate hosts... plain old fashion common word queries.

Sample Slides. Show up for all-new Blackhat Goodness!

Lame Automated Crawling

These queries ‘trip up’ the Google domain search, giving so many results...

Sample Slides. Show up for all-new Blackhat Goodness!

digital self defense
Lame Automated Crawling

Sample Slides. Show up for all new Blackhat Goodness!

Sweet Automated Crawling

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense
Googleturd Domain Scrapping

Let's say we're looking at NASA...

We can use "google turd" searches, like site:vasa to locate types which may be useful...

What's missing from these names?

Host verification...

- Let's fix the names and resolve them...

Terminal — bash — 84x14

We can further expand on these IP ranges via DNS queries as well...

Pay dirt!!!

Sample Slides. Show up for all-new Blackhat Goodness!

digital self defense
Armed With Names. Now what?

- Once we get a nice juicy list of DNS and domain names, what can we do with them?
  - Expand on our list to find more targets.
  - Map the list using standard network tools.
  - Determine external relationships to other targets.

Sample Slides. Show up for all-new Blackhat Goodness!

Expanding a target list

- If we've got a list of known good names, we can expand that list in a few ways:
  - DNS prediction with Google
  - Basic fuzzing

Sample Slides. Show up for all-new Blackhat Goodness!

digital self defense
Basic Fuzzing

- Given hosts with numbers and "predictable" names, we could fuzz the numbers, performing DNS lookups on those names...
- I'll let Roelof at sensepost discuss this topic, however... =)
DMS Prediction With Google

- From whatever source, let's say we get two names from Verizon, 'foundation' and 'investor'...

Sample Slides. Show up for all new Blackhat Goodness!

---

digital self defense
Expanding DNS Prediction

- Then, we can take all these words and perform DNS host lookups against each of these combinations:

---

digital self defense
**Digital Self Defense**
Sample Slides. Show up for all-new Blackhat Goodness!

**DNS Prediction - Vitality**

Basic DNS check confirms the hosts are live. Web servers Google didn't know about.

**DNS Prediction - Results**

<table>
<thead>
<tr>
<th>Predicted DNS Name</th>
<th>Results from site query</th>
<th>Up/Down?</th>
</tr>
</thead>
<tbody>
<tr>
<td>engineering.univ.abc</td>
<td>6,370</td>
<td>Up</td>
</tr>
<tr>
<td>geography.stat.edu</td>
<td>3,079</td>
<td>Up</td>
</tr>
<tr>
<td>acc.edu</td>
<td>9,578</td>
<td>Up</td>
</tr>
<tr>
<td>psychology.stat.edu</td>
<td>315</td>
<td>Up</td>
</tr>
<tr>
<td>nursing.stat.edu</td>
<td>18</td>
<td>Up</td>
</tr>
<tr>
<td>hospitality.stat.edu</td>
<td>12</td>
<td>Up</td>
</tr>
<tr>
<td>library.stat.edu</td>
<td>13</td>
<td>Down</td>
</tr>
<tr>
<td>business.stat.edu</td>
<td>5</td>
<td>Up</td>
</tr>
<tr>
<td>education.stat.edu</td>
<td>5</td>
<td>Down</td>
</tr>
</tbody>
</table>

13 new predicted hosts, 7 new, 4 missing web servers.

Sample Slides. Show up for all-new Blackhat Goodness!

digital self defense
Limitless mapping possibilities...

- Once you get rolling with Google mapping, especially automated recursive mapping, you’ll be ABDAZED at how deep you can dig into the layout of a target net.

Sample Slides. Show up for all new Blackhat Goodness!

---

Determining Relationships

- We can expand beyond our target domain to discover (potentially weak) sites that are related to our target.
- Most systems are only as secure as their weakest link.
- If a poorly-secured company has a trust relationship with your target, that’s your way in.
- We have some decent options for determining relationships:
  - Raw Google Link usage
  - Rule-based link extraction and weighing

Sample Slides. Show up for all new Blackhat Goodness!
Link shows Google ranks, not relationships...

Knowing that these sites link to www.microsoft.com is great, but how relevant is the information?

Do we necessarily care about Google-ranked relationships? How do we get to REAL relationships?

Sample Slides. Show up for all new Blackhat Goodness!

Non-obvious site relationships

- Sensepost to the rescue again! =)
- BILE (the Bi-directional Link Extractor), available from http://www.sensepost.com/garage_portal.html helps us gather together links from Google and piece together these relationships.
- There's much more detail on this process in their whitepaper, but in short, BILE weights the relationships of sites found in Google using specific weighing rules.

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense
Over-simplified BiLE rules

- A link from a site weighs more than a link to a site.
- A link from a site with a lot of links weighs less than a link from a site with a small amount of links.
- A link to a site with a lot of links to the site weighs less than a link to a site with a small amount of links to the site.
- The site that was given as input parameter need not end up with the highest weight— a good indication that the provided site is not the central site of the organization.

Sample Slides: Show up for all-new Blackhat Goodness!

Example: Who is Sensepost?

Let's pretend we don't know who Sensepost is.

Relying on Google's 6400+ sites, he can be daunting...and misleading.

Sample Slides: Show up for all-new Blackhat Goodness!

digital self defense
**BiLE: www.sensepost.com**

* Let's point BiLE at www.sensepost.com...

Sample Slides. Show up for all-new Blackhat Goodness!

---

* Next, BiLE takes the output from the extraction phase...

Sample Slides. Show up for all-new Blackhat Goodness!

---

**digital self defense**
Document Grinding and Database Digging

Documents and databases contain a wealth of information. Let’s look at ways to take advantage of SQL databases with Google.

Sample Slides: Show up for all new Blackhat Goodness!

SQL Usernames

"Access denied for user "being password"

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

digital self defense
**SQL Schemas**

- Entire SQL database dumps

---

**SQL injection hints**

- Improper command termination can be avoided quite easily by an attacker.

---

*Samples only! Show up for the good stuff!*

---

digital self defense
**SQL source**

- Getting lines of SQL source can aid an attacker.

```
SELECT user_id, password FROM users WHERE email = 'example@email.com';
```

******* SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *******

---

**Going after SQL passwords**

```
filetype:html in:domain:sql\connect
```

Include files with cleartext passwords...

******* SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *******

---

digital self defense
More SQL Passwords

- Question: What's the SQL syntax that can be used to set a password?
- (TWO WORDS)

- One Answer: "Identified by"

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

More SQL Passwords

- The slightly more hardcore version...

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

digital self defense
Various database detection queries

<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SELECT * FROM</td>
<td>WHERE ID = 123</td>
</tr>
<tr>
<td>SELECT DISTINCT</td>
<td>ID FROM table1 WHERE ID = 456</td>
</tr>
<tr>
<td>SELECT COUNT(*)</td>
<td>FROM table2 WHERE ID = 789</td>
</tr>
<tr>
<td>SELECT MAX(price)</td>
<td>FROM products WHERE category = 'Electronics'</td>
</tr>
<tr>
<td>SELECT AVG(age)</td>
<td>FROM employees WHERE department = 'Sales'</td>
</tr>
</tbody>
</table>

SQL Dump detection

Database detection

******** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! ********

Automation

Page Scrolling in PDF

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense
Page Scraping with Perl

- This Perl code, by James Foster, provides a good framework for "page scraping" Google results.
- This method relies on manually querying Google, and searching the resultant HTML for the "interesting stuff."

We will be making socket calls. We need IO::Socket.

We hardcode our query (which we can make parameterized), our Google search and our parameters.

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense
Page Scraping with Perl

This subroutine declares the Google query (hard-coded above) and accepts one parameter, the Google query.

Google returned HTML is processed, and the line containing "of about" (along with line) is returned from the routine.

Sample Slides. Show up for all-new Blackhat Goodness!

---

Page Scraping with Perl

This subroutine takes one parameter (the result line from the Google query).

...of/about is located...

...the next 30 characters are grabbed...

...all the digits are removed...

...stared in $site...

...and returned...

Sample Slides. Show up for all-new Blackhat Goodness!

---

digital self defense
Page Scraping with Perl

Sample Slides. Show up for all new Blackhat Goodness!

Web Servers, Login Portals, Network Hardware

Network devices can be a good search item to Google for...

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

* digital self defense
Web File Browser

- This program allows directory walking, file uploading, and more.

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

VNC Servers (with client)

- VNC (Virtual Network Computing) allows you to control a workstation remotely.

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

digital self defense
Symantec Anti-Virus SMTP Gateways

SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! ****

Axis Print Servers

SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! ****

digital self defense
**Xenix, Swook, Orite Web Cams**

One query, many hundreds of livecams!

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

---

**Active WebCam**

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

---

digital self defense
Toshiba Network Cameras

SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF!

Speedstream DSL Routers

- Home broadband connectivity... Googled.

SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF!

digital self defense
Belkin Routers

- Belkin routers have become a household name in connected households. The management interface shouldn't show up on Google... but it does.

Network Utilities

WebUtil Version: 3.7

One query, lots of tools...

digital self defense
**Microsoft Virtual Server 2006**

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

---

**Printers**

- Trolling printers through Google can be fun, especially when you can see and download what others are printing...

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

---

'digital self defense'
More printer fun!

The things you can do with a printer are just amazin'. Look at all these settings...

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

digital self defense
digital self defense
Firewalls - IPCop

Okay...this one needs updating too!

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

IDS Data: ACID

- SNORT IDS data delivered graphically, served up fresh

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

digital self defense
Open Cisco Devices

Switch

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

Cisco Switches

Cisco Systems

Accessing Cisco WS-C3550-48 "Switch"

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****
digital self defense
Wide Open PHP Nuke Sites

- PHP Nuke allows for the creation of a full-featured website with little effort.

Open PHP Nuke... another way...

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****
Security Cameras

- Although many cameras are multi-purpose, certain brands tend to be used more for security work.
Time-lapse video recorders

- A staple of any decent security system, these camera control units have gotten high-tech. And Googleable...

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

---

digital self defense
digital self defense
Haeking POWER Systems!

- Ain't technology grand? This product allows web management of power outlets!

Google search located login page. What does a google search do to a login page?

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

---

Haeking Power Systems!

Who do you want to power off today?

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

digital self defense
digital self defense
Google Phreaking

- Question... Which is easier to hack with a web browser?

A: Sipura SPA 2000 IP Telephone
B: Vintage 1970's Rotary Phone

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

---

Sipura SPA IP Telephone

How about Googleing for the best modem router in the world today?

Or the best modem that didn't die?

Theres dimensions!

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

digital self defense
Videoconferencing

PBX Systems

- Web-based management interfaces open the door for a creative Google Hacker.

*Note:* For samples only! Show up for the good stuff!

digital self defense
PBX Systems

Usersnames, Passwords and Secret Stuff, oh my!

There's all sorts of stuff out there that people probably didn't mean to make public. Let's take a look at some examples...

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****
digital self defense
Old School! Finger...

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

digital self defense
Open SQL servers

Already logged in, no logging required!

***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

ServU FTP Passwords

ServU FTP
Username: super
Password: P

Thanks to
out with the bad...
digital self defense
Police Reports...

Sensitive Government Documents

- Question: Are sensitive, non-public Government documents on the web?
- Answer: Yes.

digital self defense
Sensitive Government Documents

- Placeholder. Show up for the real goods!

Sample Slides. Show up for all-new Blackhat Goodness!

Social Security Numbers

- Placeholder. Show up for the real goods!

Sample Slides. Show up for all-new Blackhat Goodness!

digital self defense
Credit Cards!

• Placeholder. Show up for the real goods!

Sample Slides. Show up for all new Blackhat Goodness!

Super Secret Stuff!

• This section too hot for print! Show up to the talk or miss out! =)}

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense
What we've done...

- We've skimmed "Google Hacking for Penetration Testers" by Syngress Publishing, which doesn't seem to suck.
- We've looked at some great tools by Roelof Temmingh. Check out Sensepost.com.
- We've invaded the privacy of millions.
- We're all still awake. Right?

Sample Slides. Show up for all new Blackhat Goodness!

---

Thanks!

- Thanks to God for the gift of life.
- Thanks to my family for the gift of love.
- Thanks to my friends for filling in the blanks.
- Thanks to the moderators at ihackstuff.com: Murtle, Jimmy Neutron, ThePsyko, Wasabi, Dom, Stonersavant
- Thanks to Roelof T for the great code, and to the current Google Masters: murtle, jimmyneutron, kloow, Dom, Stonersavant, MILKMAN, ThePsyko, cybercide, yseains, wolfeo, Deadline, crash_monkey, zoro25, digital_revolution, Renegade334, wasabi, urban, std, mlynch, Peedy, Vipsta, hoAcces, brasileiro, john, ZinCh

Sample Slides. Show up for all new Blackhat Goodness!

digital self defense