

Johnny Long

CSC



BLACK HAT BRIEFINGS

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 foot 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 ("Yarrrrr!"), 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
jlong@hacks.kitfox.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 G

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!

Advanced Operators at a Glance

Advanced operators can be combined in some cases.

In other cases, mixing should be avoided.

Operator	Purpose	Use w/ other operators	Can be used alone?	Does search work?			
				With	Single	Google	Meta
file	Search page file	yes	yes	yes	yes	yes	yes
urlfile	Search page file	no	yes	yes	yes	yes	yes
url	Search URL	yes	yes	yes	yes	not really	file title
urlurl	Search URL	no	yes	yes	yes	yes	file title
sitefile	Search specific file	yes	no	yes	yes	no	not really
urlfileurl	Search from url of page only	not really	yes	yes	yes	yes	yes
file	Search specific file	yes	yes	yes	yes	no	not really
url	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
number	Search for number	yes	yes	yes	no	no	not really
urlnumber	Search for number in URL	yes	no	yes	not really	not really	not really
author	Search for author search	yes	yes	no	no	yes	not really
group	Search for group search	not really	yes	no	no	yes	not really
inanchor	Search for anchor search	yes	yes	file title	file title	yes	file title
url	Search for url search	no	yes	not really	not really	not really	not really

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

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

Crash course in advanced operators

Some operators search overlapping areas. Consider site, inurl and filetype.



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

Advanced Google Searching

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

filetype:ppt inurl:johnny.blackstaff.com

intext:johnny.blackstaff.com inrange:99999-100000

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

Advanced Google Searching

Put these individual queries together into one advanced query and you only get that one specific result.

Adding advanced operators reduces the number of results asking for us to the search.

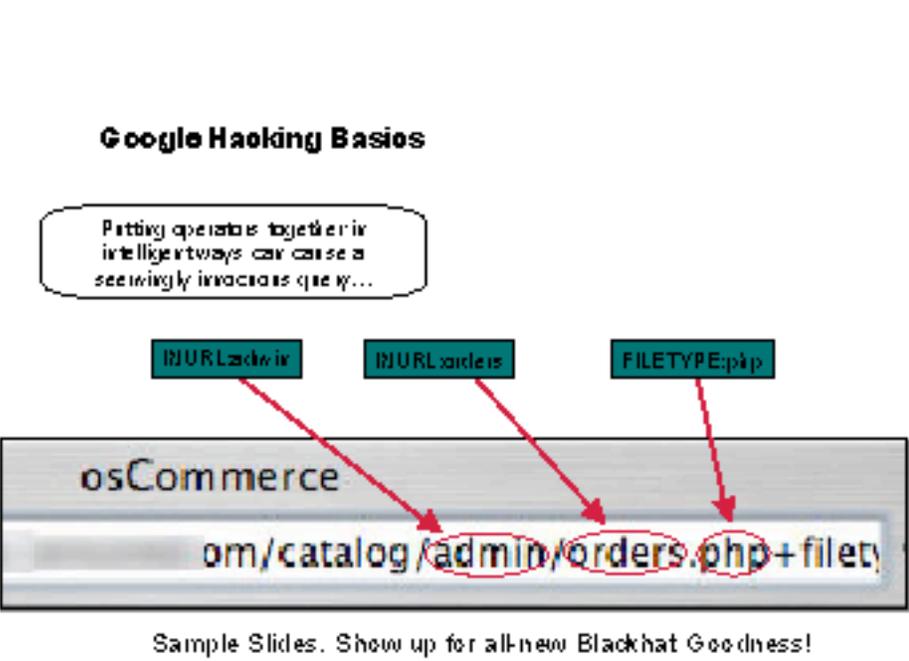
Google Hacking Basics

Putting operators together in intelligent ways can cause a seemingly innocuous query...

`INURL:dir` `INURL:orders` `FILETYPE:php`

osCommerce
`om/catalog/admin/orders.php+filet`

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



Google Hacking Basics

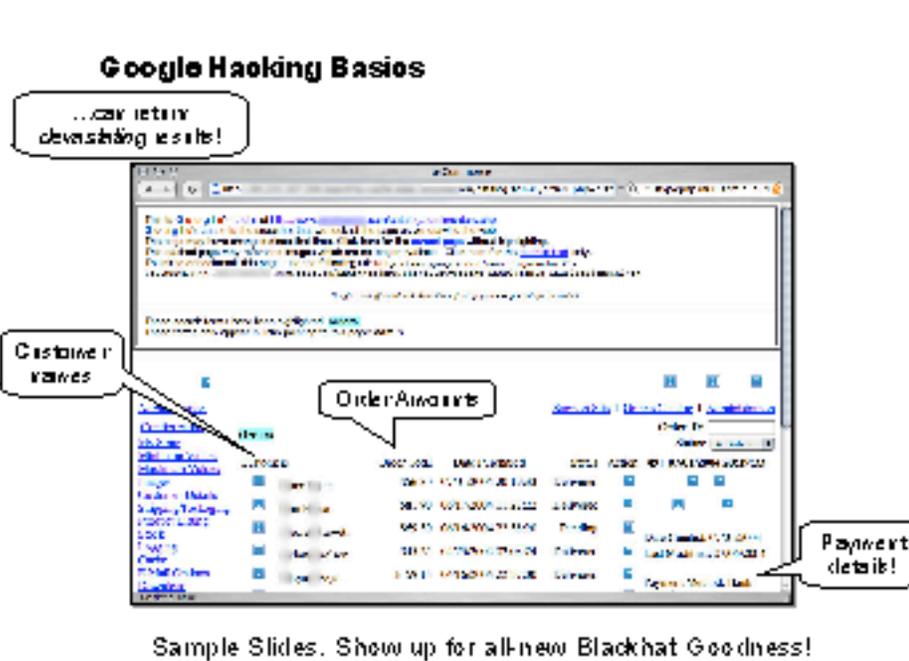
...can return devastating results!

Customer names

Order Amounts

Payment details!

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



Customer Name	Order Amount	Payment Details
John Doe	\$123.45	1234567890
Jane Smith	\$456.78	0987654321
Bob Johnson	\$789.01	1122334455
Alice Brown	\$234.56	6677889900
Charlie White	\$567.89	3344556677
Diana Green	\$890.12	9988776655
Frank Black	\$123.45	2233445566
Grace King	\$456.78	7788990011
Henry Lee	\$789.01	4455667788
Ivy Park	\$234.56	1122334455

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



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

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!

Anonymous Googling

This iptables output shows our network traffic while locating that cached page.

```
21:38:24.694623 IP 157.140.2.51:80 > 69.23.167.100:80
21:38:24.715667 IP 69.23.167.100:80 > 157.140.2.51:80
21:38:24.736351 IP 69.23.167.100:80 > 157.140.2.51:80
21:38:24.751593 IP 157.140.2.51:80 > 69.23.167.100:80
21:38:24.772587 IP 157.140.2.51:80 > 72.165.253.125:80
21:38:24.793461 IP 157.140.2.51:80 > 72.165.253.125:80
21:38:24.814216 IP 157.140.2.51:80 > 72.165.253.125:80
21:38:24.837903 IP 157.140.2.51:80 > 72.165.253.125:80
21:38:25.017267 IP 72.165.253.125:80 > 157.140.2.51:80
21:38:25.031111 IP 72.165.253.125:80 > 157.140.2.51:80
21:38:25.045028 IP 157.140.2.51:80 > 72.165.253.125:80
21:38:25.058371 IP 72.165.253.125:80 > 157.140.2.51:80
21:38:25.072337 IP 72.165.253.125:80 > 157.140.2.51:80
21:38:25.086736 IP 157.140.2.51:80 > 72.165.253.125:80
21:38:25.100417 IP 72.165.253.125:80 > 157.140.2.51:80
21:38:25.114673 IP 72.165.253.125:80 > 157.140.2.51:80
21:38:25.128702 IP 157.140.2.51:80 > 72.165.253.125:80
21:38:25.142823 IP 72.165.253.125:80 > 157.140.2.51:80
```

This is Google.

This is Pirack.

We tracked Pirack's web server. We're not anonymous.

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

Anonymous Googling

This time, the entire conversation was between us (192.168.232) and Google (64.233.167.104)

```
2048:50050067 BY 192.168.232.10212 > 64.233.167.104
2048:50050077 BY 64.233.167.104 > 192.168.232.10212
2048:50050085 BY 192.168.232.10212 > 64.233.167.104
2048:50050095 BY 192.168.232.10212 > 64.233.167.104
2048:50050107 BY 64.233.167.104 > 192.168.232.10212
2048:50129050 BY 64.233.167.104 > 192.168.232.10212
2048:50129062 BY 64.233.167.104 > 192.168.232.10212
2048:50129075 BY 64.233.167.104 > 192.168.232.10212
2048:50129087 BY 64.233.167.104 > 192.168.232.10212
2048:50129100 BY 192.168.232.10212 > 64.233.167.104
2048:50129112 BY 192.168.232.10212 > 64.233.167.104
2048:50129125 BY 64.233.167.104 > 192.168.232.10212
2048:50129137 BY 64.233.167.104 > 192.168.232.10212
```

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

Anonymous Googling

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

- Original:

```
http://64.233.167.104/used/?m=vid:s27FrsDbbdEwww.giendkregiufatm-wf2fyiendeh  
sufom-wf2&hl=en
```

- Cached Text Only:

```
http://64.233.167.104/used/?m=vid:s27FrsDbbdEwww.giendkregiufatm-wf2fyiendeh  
sufom-wf2&hl=en&strip=1
```

Adding `&strip=1` to the end of the cached URL only shows Google's text, not the targets.

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.



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

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 something *cat+war*
 - (-) exclude a search term
 - (") use quotes around search phrases
 - (.) a single-character wildcard
 - (*) any word
 - (|) boolean 'OR'
 - Parenthesis is group queries (*waste card*) | *waste card*)

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

Introducing the GoogleDork Detection System! (GDDS)

- Google has started blocking queries, most likely as a result of worms that slam 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?q=inurl:*.php&rlz=3C1w%20n%5=L&oeq=L0&oeq=0
```

- Stripped down, the query looks like this:

```
http://www.google.com/search?q=inurl:*.php&oeq=L0
```

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

```
http://www.google.com/search?q=inurl:*.PHP&oeq=L0
```

```
http://www.google.com/search?q=inurl:*.PHp&oeq=L0
```

```
http://www.google.com/search?q=inurl:*.Ph&oeq=L0
```

Sample Slides. Show up for all-new Blackhat Goodness!
This works in the Web interface as well.

BLACKHAT BRIEFINGS

Bypassing GDS Round 2 - Query Shifting

The top screenshot shows a Google search for 'int:index.php' resulting in a 'We're sorry...' error page. A callout bubble points to the search bar with the text 'int:index.php is blocked.' The bottom screenshot shows the same search query converted to 'filetype:pdf int:index.php', which successfully returns search results. A callout bubble points to the search bar with the text 'Query converted into filetype and phrase search'.

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

Bypassing GDS Round 3: Space / + injection

The top screenshot shows a Google search for 'int:index.php' resulting in a 'We're sorry...' error page. A callout bubble points to the search bar with the text 'Phrase blocked'. The bottom screenshot shows the search query 'int:index.php' with a space character injected, resulting in a successful search result. A callout bubble points to the search bar with the text 'Use it spaces (or + signs in url)...'. Another callout bubble points to the search bar with the text '...query works.'.

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 would 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 precedent.

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

Pre-Assessment

There are many things to consider before listing a target, many of which Google can help with. One striking example is the collection of email addresses and usernames.

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

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 a lynx to automate the download of the search results:

```
lynx -dump https://www.google.com/search?q=@gmail.com >results.txt
```

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

```
([a-zA-Z0-9_-]+@[a-zA-Z0-9_-]{1,25}\.[a-zA-Z]{2,4})|([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})
```

- 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:



It searches the first 10 Google results... with only one hit against your API key.

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

More Email Automation

Running the tool through 50 results (with a 5 per page limit instead of 1) finds even more addresses.

un@domain1.com
f@domain1.com
b@domain1.com
b@domain1.com
d@domain1.com
l@domain1.com
j@domain1.com
v@domain1.com
e@domain1.com
j@domain1.com
s@domain1.com
g@domain1.com
p@domain1.com
b@domain1.com
i@domain1.com
f@domain1.com
e@domain1.com
n@domain1.com
m@domain1.com
a@domain1.com
l@domain1.com
f@domain1.com
s@domain1.com
a@domain1.com
a@domain1.com
m@domain1.com
k@domain1.com
j@domain1.com
j@domain1.com

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

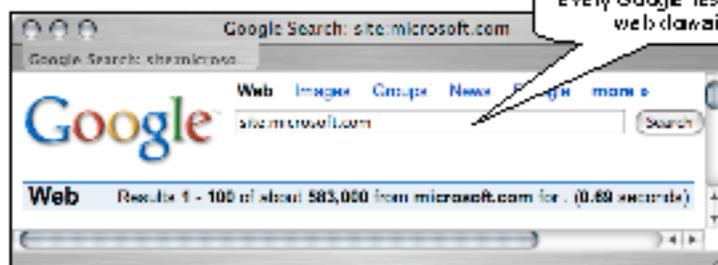
Network Mapping

Google is an invaluable tool for mapping out an Internet-connected network.
Let's look at ways Google can help its cover targets and map out networks.

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

Basic Domain Crawling

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



Sample Slides. Show up for all-new Blackhat Goodness!
[site: microsoft.com](http://site:microsoft.com)

Basic Domain Crawling



Klasi on v, a site search makes the obvious stuff float to the top.

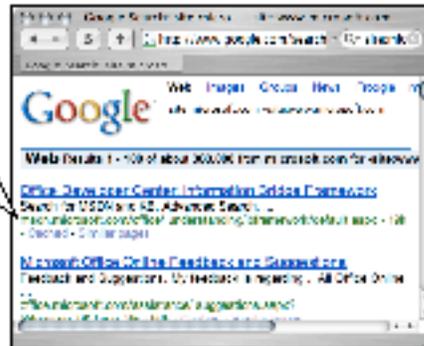
As a security tester, we need to get to the less obvious stuff.

www.microsoft.com is way too obvious...

Basic Domain Filter

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

Notice that the obvious "www" is missing, replaced by more interesting domains.



site:microsoft.com
-site:www.microsoft.com

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

Ugly Domain Filtering

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

```
~!bz:wicn:icrn:ft:om  
~!bz:innn:icrn:ft:om  
~!bz:wdr:icrn:ft:om  
~!bz:up:icrn:ft:om  
~!bz:drrn:icrn:ft:om  
~!bz:ff:icrn:ft:om  
...
```

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...

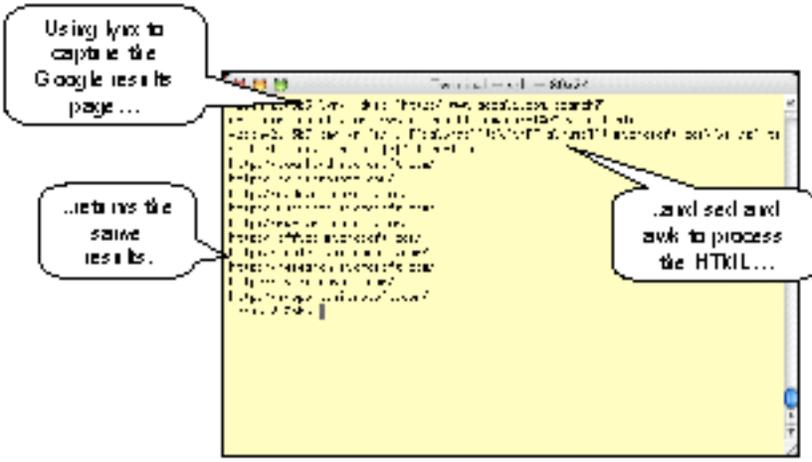
Research page ...

HTTPS page ...

Eventually we'll run into a 32 query limit, and this process tends to be tedious.

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

Better Domain Crawling



Using lynx to capture the Google results page ...

```
www.mozilla.com: 68.142.250.100: www.mozilla.com?
```

...returns the same results.

...and send awk to process the HTKIL...

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

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 floats to the top. Some more "interesting stuff" trolls near the bottom.
 - "Hints" for follow-up recon. 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!

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!

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... =)



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

Using Google to find hosts Google doesn't even know about!

- Question: Can Google be used to locate hosts that Google doesn't even know about?
- Answer: Yes
- Question: Can anyone name a specific tool developed just for this reason?

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

Limitless mapping possibilities...

- Once you get rolling with Google mapping, especially automated recursive mapping, you'll be AMAZED 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

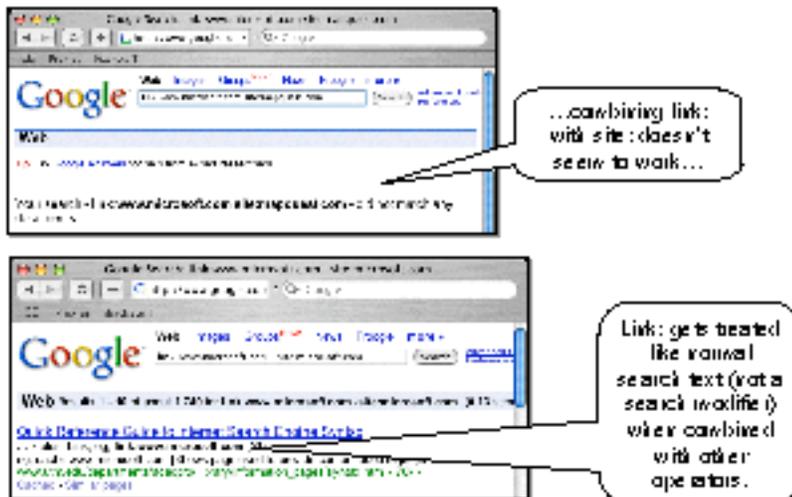
Sample Slides. Show up for all-new Blackhat Goodness!

Raw Link Usage



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

Link has limits



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

Link shows Google ranks, not relationships...

Knowing that these sites link to www.wicrsoft.com is great, but how relevant is this 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!

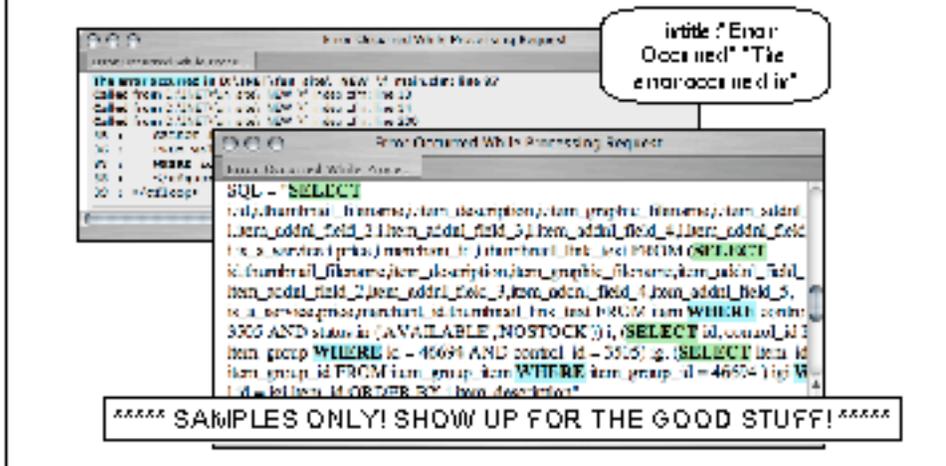
Non-obvious site relationships

- 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 weighs the relationships of sites found in Google using specific weighing rules.

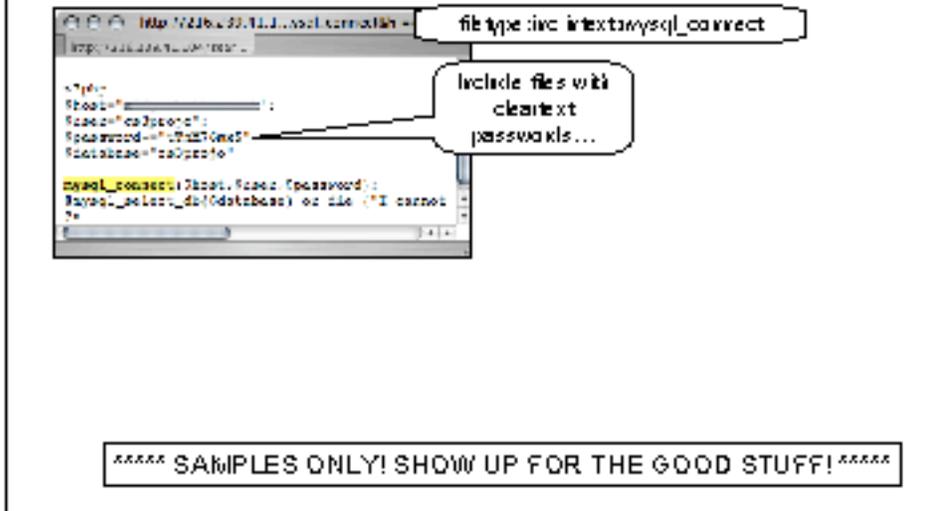
Sample Slides. Show up for all-new Blackhat Goodness!

SQL source

- Getting lines of SQL source can aid an attacker.



Going after SQL passwords



More SQL Passwords

- Question: What's the SQL syntax that can be used to set a passwords?
- (TWO WORDS)
- One Answer: "Identified by"

Q: filetype:sql = IDENTIFIED BY -aa



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

More SQL Passwords

- The slightly more hardcore version...

Q: filetype:sql = IDENTIFIED BY ("Grant" on " | create user")



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

Various database detection queries

Query	Description
mysql://[username]@[hostname]:[port]/[database]	mysql://[username]@[hostname]:[port]/[database]

SQL dump detector

Query	Description
mysql://[username]@[hostname]:[port]/[database]	mysql://[username]@[hostname]:[port]/[database]

Database detector

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

Automation

Page Scraping in Perl

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

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."

```
#!usr/bin/perl -w
use IO::Socket;

my $url = "http://www.google.com/";
my $port = 80;
```

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

We hardcode as many as possible (which we can make a parameter later), our Google search URL as a parameter.

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

Page Scraping with Perl

```
my $url = "http://www.google.com/";
my $port = 80;

my $socket = IO::Socket::INET->new(
    PeerAddr => $url,
    PeerPort => $port,
    Protocol => "tcp",
    Listen => 5,
);

my $response = $socket->recv(1024);
my $html = $response->[0];

my $content = $html->[0];
```

Next we have a very generic socket initialization subroutine.

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

Page Scraping with Perl

```

my $url = "http://www.google.com/search?q=James+Foster&btnG=Google+Search";
my $response = HTTP::Get($url);
my $html = $response->content();
my $url = "http://www.google.com/search?q=James+Foster&btnG=Google+Search";
my $response = HTTP::Get($url);
my $html = $response->content();
my $url = "http://www.google.com/search?q=James+Foster&btnG=Google+Search";
my $response = HTTP::Get($url);
my $html = $response->content();

```

This subroutine sends the Google query (as located above) and accepts one parameter, the Google query.

Google returned HTML is processed, and the line containing "of about" (or less) is returned from this routine.

Results 1 - 10 of about 46,600 for "James Foster". (0.49 seconds)
Sample Slides. Show up for all-new Blackhat Goodness!

Page Scraping with Perl

```

my $url = "http://www.google.com/search?q=James+Foster&btnG=Google+Search";
my $response = HTTP::Get($url);
my $html = $response->content();
my $url = "http://www.google.com/search?q=James+Foster&btnG=Google+Search";
my $response = HTTP::Get($url);
my $html = $response->content();
my $url = "http://www.google.com/search?q=James+Foster&btnG=Google+Search";
my $response = HTTP::Get($url);
my $html = $response->content();

```

This subroutine takes one parameter (the results line from the Serch query)

"of about" is located...

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

...all the digits are removed...

...stored in \$site...

...and returned.

Results 1 - 10 of about 46,600 for "James Foster". (0.49 seconds)
Sample Slides. Show up for all-new Blackhat Goodness!

BLACKHAT BRIEFINGS

Page Scraping with Perl

```
#!/usr/bin/perl
use LWP::Simple;
my $url = "http://www.google.com";
my $agent = "Mozilla/5.0 (X11; Linux i686; rv:1.9.0.1) Gecko/20080702 Firefox/3.0";

my $html = get($url, $agent);

my $total = $html =~ /total: (\d+)/;

print $total;
```

The socket is initialized...

...the query is sent...

This piece of code drives all the subroutines.

...the total is determined...

...and print it out.

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

Web Servers, Login Portals, Network Hardware

Network hardware can be 5000 worth fun to Google for...

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

Web File Browser

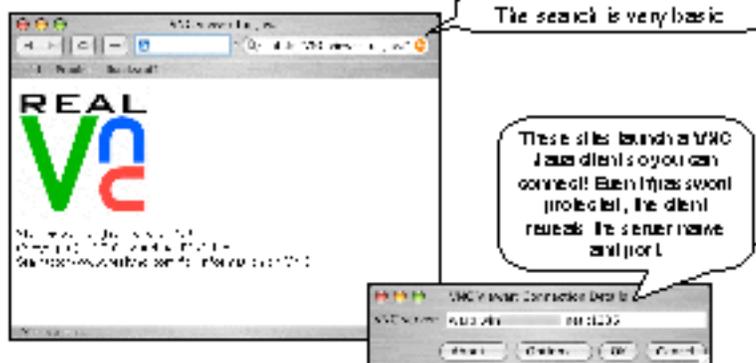
- This program allows directory walking, file uploading, and more.



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

VNC Servers (with client)

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



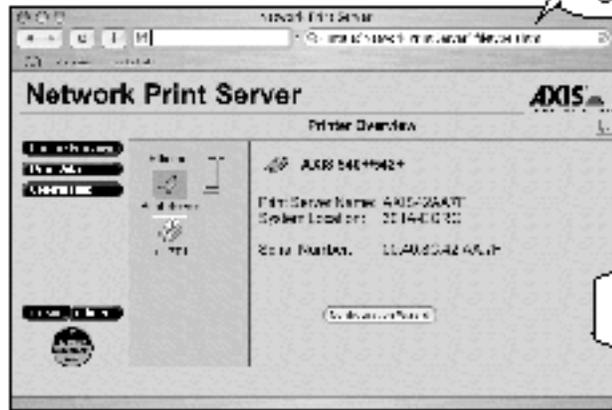
***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

Symantec Anti-Virus SMTP Gateways



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

Axis Print Servers



Print server administration, Google-style!

Thanks to thanks for feedback

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

Xenix, Sweex, Orite Web Cams



One query, many brands of live cams!

Thanks to search for fiberopt

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

Active WebCam



Thanks to search

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

Toshiba Network Cameras



A screenshot of a web browser window titled "TOSHIBA Network Camera - User Login". The browser's address bar shows "http://192.168.1.100:8080/". The page has a blue header with the "TOSHIBA" logo and a "Welcome Message" section with "OK" and "Cancel" buttons. Below this is a video feed showing an outdoor scene with a road and trees. A speech bubble points to the browser title bar with the text "in title: 'toshiba network camera - User Login'". A callout box at the bottom right says "Fixed by WebCrew".

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

Speedstream DSL Routers

- Home broadband connectivity... Googled.



A screenshot of a web browser window showing the "Speedstream Router Management Interface". The browser's address bar shows "http://192.168.1.100:8080/". The page has a blue header with the "SpeedStream" logo and "Efficient" branding. Below this is a "System Summary" section with the following details: "System type: Speedstream DSL Router", "Config Part#: 001-0145-010", "Firmware Part#: 004-0101-012", and "MAC Address: 08152004 0100". A speech bubble points to the "System Summary" section with the text "Who do you want to disconnect today?". A callout box at the bottom right says "Fixed by WiFi".

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

Belkin Routers

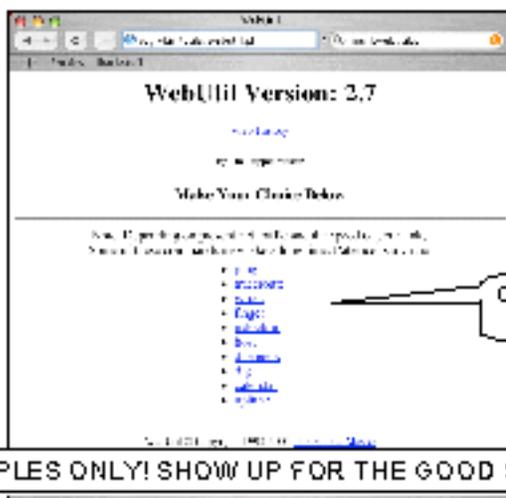
- Belkin routers have become a household name in connected households. The management interface shouldn't show up on Google... but it does.



Thanks
@stuartm

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

Network Utilities



One query, lots
of tabs ...

Thanks
@stuartm

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

Microsoft Virtual Server 2006



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

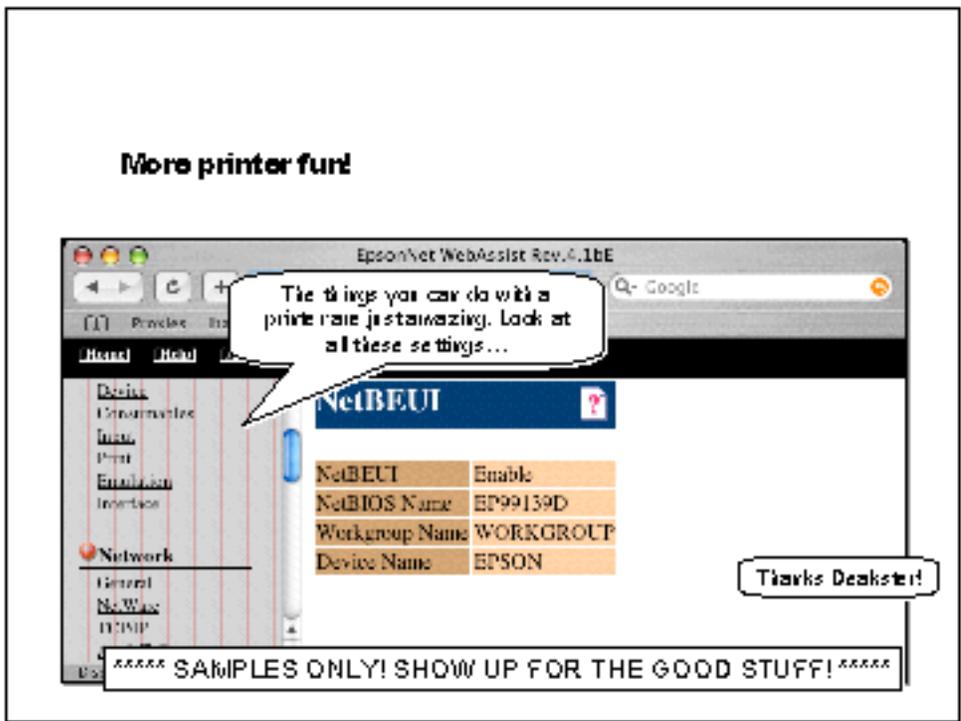
Printers

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

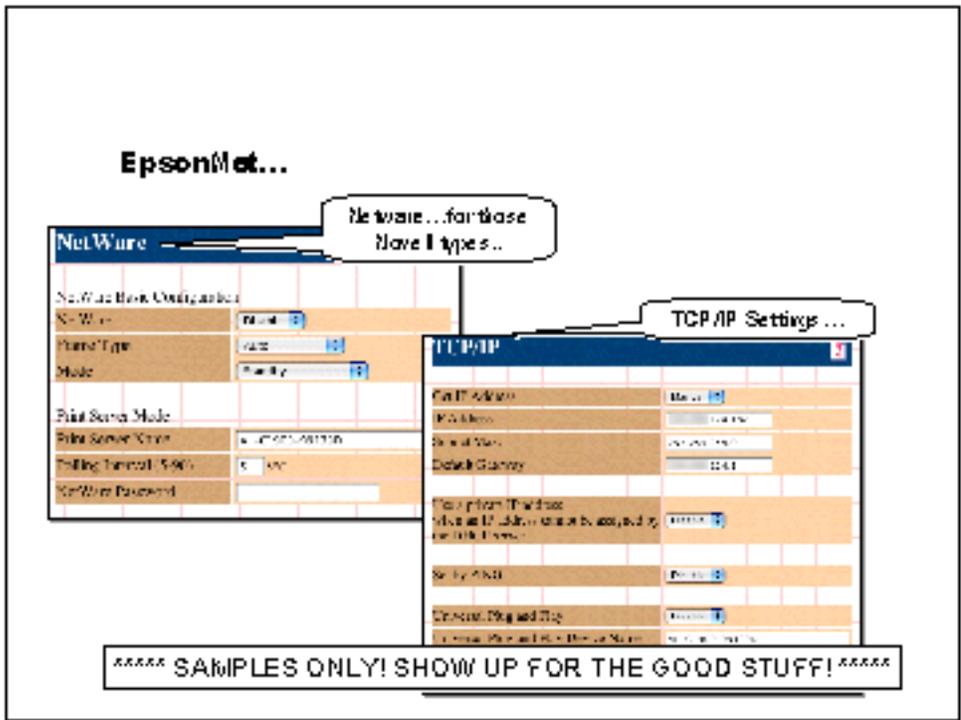


***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

More printer fun!

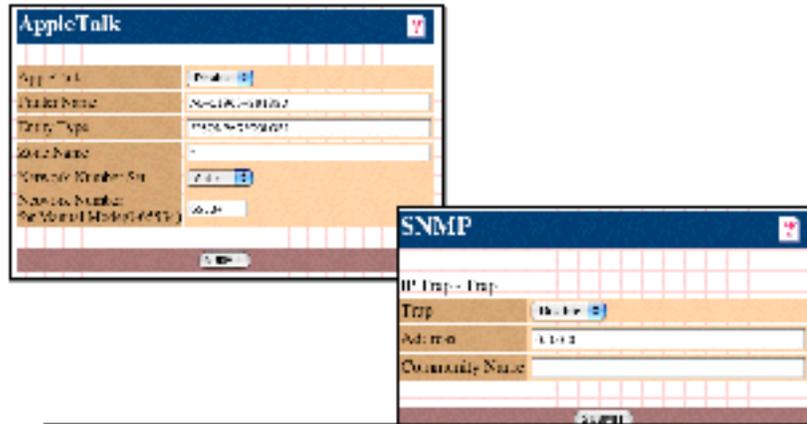


EpsonNet...



BLACK HAT BRIEFINGS

EpsonNet...



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

Firewalls - Smoothwall



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

Firewalls - IPCop

Use it... this one needs updating too!

Thanks, Jimmy Neufeld

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

The screenshot shows the IPCop website with the heading "The Bad Pockets Stop Here". A central text box contains a warning about a "Mod 5" vulnerability. A callout bubble points to a specific section of the page, and a signature box is visible in the bottom right corner.

IDS Data: ACID

- SNORT IDS data delivered graphically, served up fresh

ACID by Rowan Dwyer filetype ppt

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

The screenshot displays the ACID web interface. On the left, there is a sidebar with navigation options. The main content area shows a table of IDS data. A callout bubble points to the table, and a signature box is visible in the bottom right corner.

IP	Port	Protocol	Direction	Count	Rate
192.168.1.1	80	TCP	Outgoing	1000	1000.00
192.168.1.1	80	TCP	Incoming	500	500.00
192.168.1.1	443	TCP	Outgoing	200	200.00
192.168.1.1	443	TCP	Incoming	100	100.00
192.168.1.1	22	TCP	Outgoing	50	50.00
192.168.1.1	22	TCP	Incoming	25	25.00

BLACK HAT BRIEFINGS

Open Cisco Devices



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

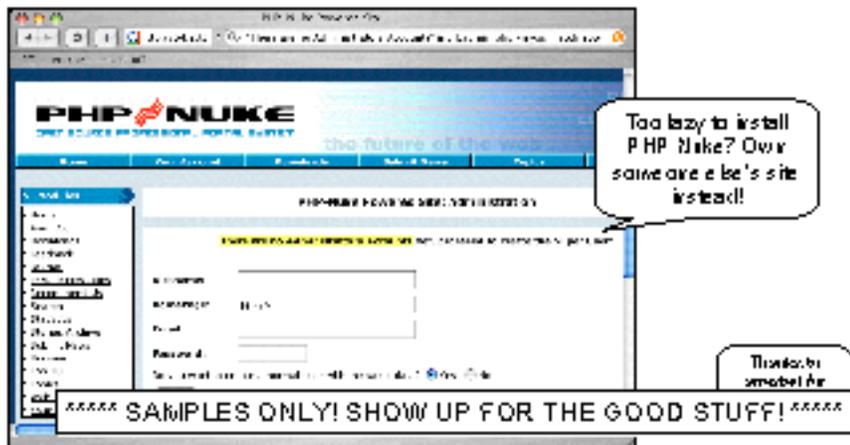
Cisco Switches



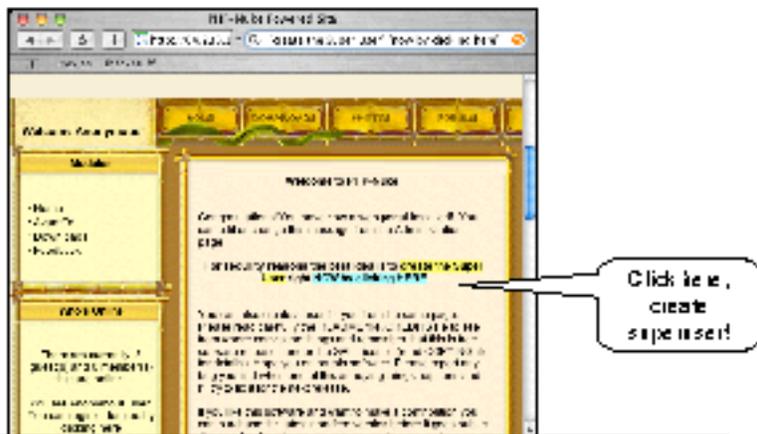
***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

Wide Open PHP Nuke Sites

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



Open PHP Nuke... another way...



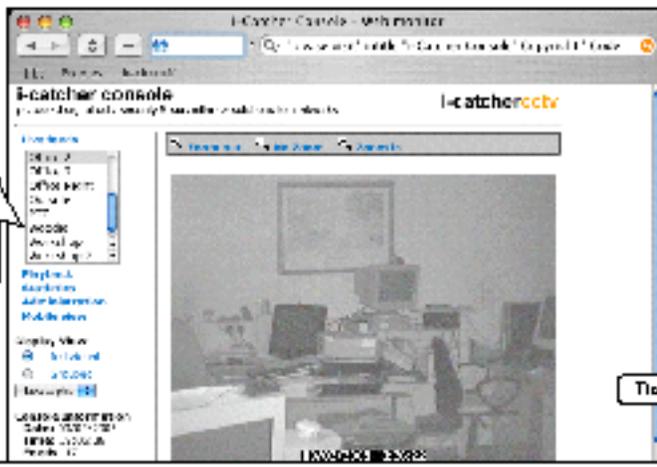
Security Cameras

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



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

Security Cameras



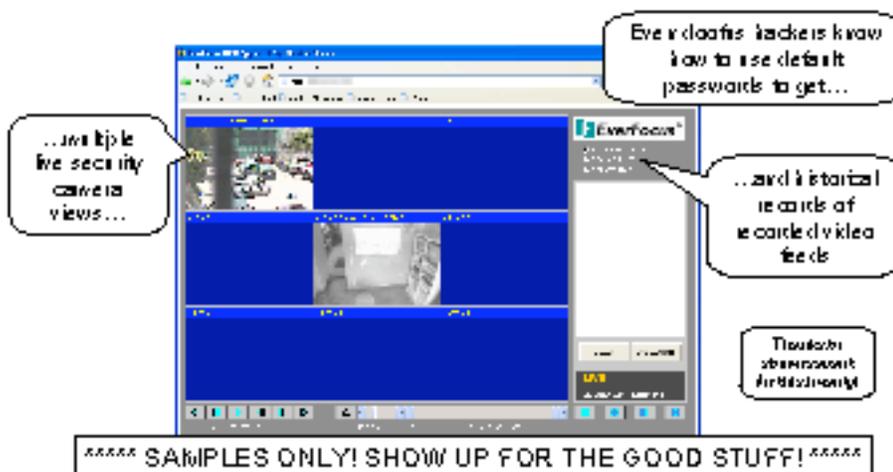
***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

Time-lapse video recorders

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



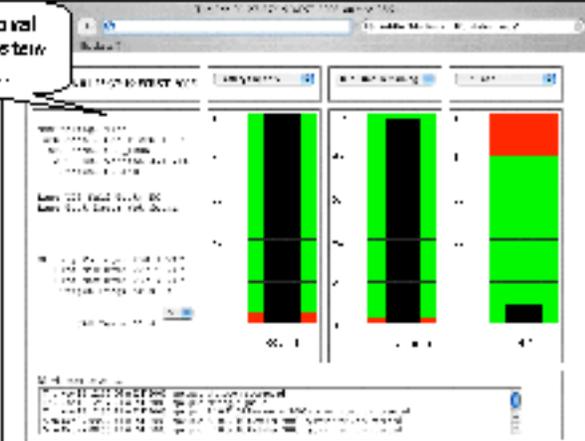
Time lapse video recorders



BLACK HAT BRIEFINGS

UPS Monitors

Getting personal with PowerSystem monitors...



Thanks, yepnot

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

Detailed description: This panel shows a screenshot of a PowerSystem UPS monitor. The interface features three vertical bar charts, each representing a different UPS unit. The bars are segmented into green and red, likely indicating operational status or battery levels. A callout bubble on the left points to the interface with the text 'Getting personal with PowerSystem monitors...'. A small box on the right says 'Thanks, yepnot'. At the bottom, a banner reads '***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****'.

UPS Monitors

Oh wait. Wrong kind of UPS...this is package tracking...=P



Thanks, Dylid Spitt

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

Detailed description: This panel shows a screenshot of a Google search results page for the query 'UPS Package Tracking'. The search results list several links to UPS tracking pages. A callout bubble on the right says 'Oh wait. Wrong kind of UPS...this is package tracking...=P'. A small box on the right says 'Thanks, Dylid Spitt'. At the bottom, a banner reads '***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****'.

Hacking POWER Systems!

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



Google search locates login page. What does any decent hacker do to a login page?

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

Hacking Power Systems!

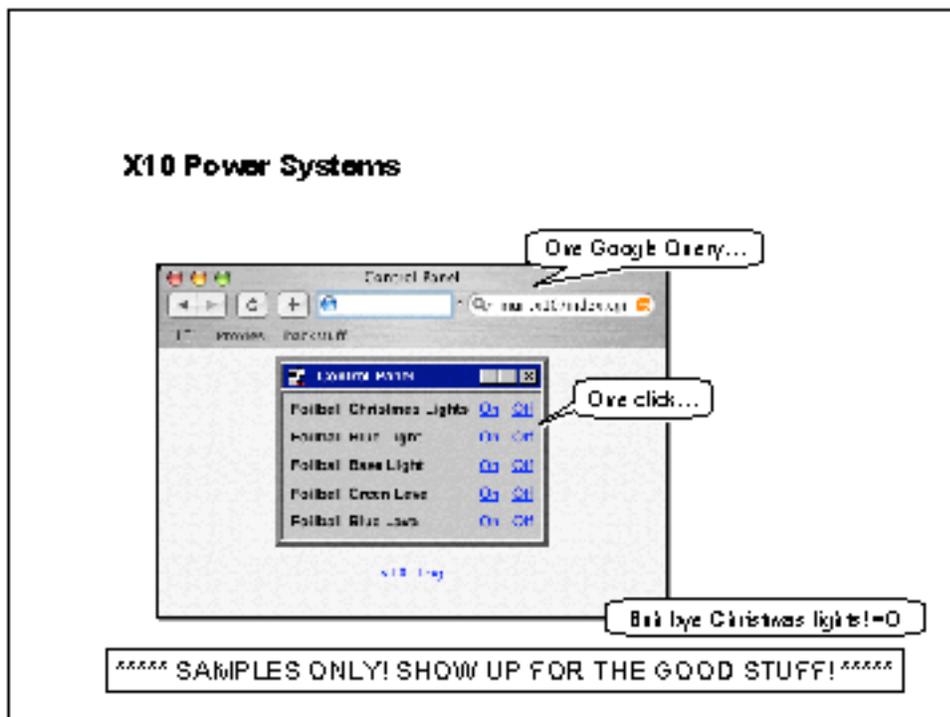
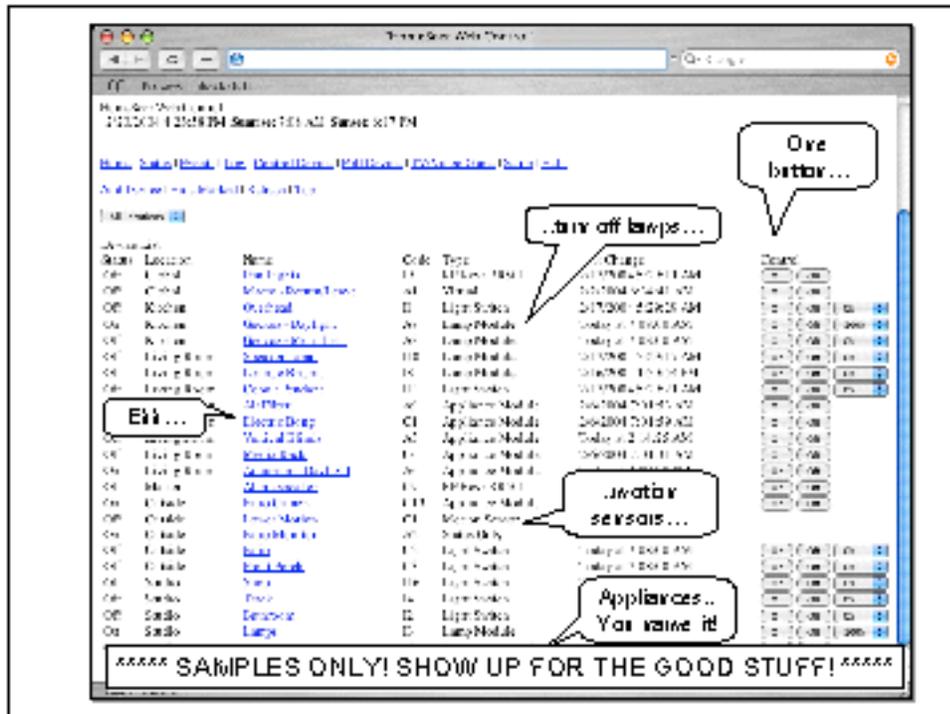


What do you want to power off today?

Thanks to Jhony@hacking for this security!

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

BLACK HAT BRIEFINGS



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 Googling for the last number in the file w/d diskid?

On the last number that diskid there?

Thanks, @stunners001!

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

PBX Systems



No password required.
Even a voice web server

There's always a list of users

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

Username, 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! *****

Old School! Finger...

Google Hacking circa 1980!?!
Thanks to Jerry Matford
***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

Morton AntiVirus Corporate Passwords

Example d, but yummy (and credible)!
Thanks KILIKIAN
***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****

Matscape History Files

Oops.. POP email passwords!

Thanks to @lightblue0x0 for the tip!

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

The screenshot shows a terminal window with a list of files and their contents. A callout bubble points to a line containing 'POP email passwords!'. Another callout bubble points to a line containing 'Thanks to @lightblue0x0 for the tip!'. At the bottom, a banner reads '***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****'.

IPSec Final Encryption Keys

Thanks KILIKILANI

Early skimmer Applied Cmpx

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

The screenshot shows a terminal window displaying the output of a command to retrieve IPSec final encryption keys. A callout bubble points to a line containing 'Thanks KILIKILANI'. Another callout bubble points to a line containing 'Early skimmer Applied Cmpx'. At the bottom, a banner reads '***** SAMPLES ONLY! SHOW UP FOR THE GOOD STUFF! *****'.

BLACK HAT BRIEFINGS

Explorer. EXPLORER!?!?

Who needs passwords, when you can just... Explore c:\winnt\system32?

What days do you want to delete today???

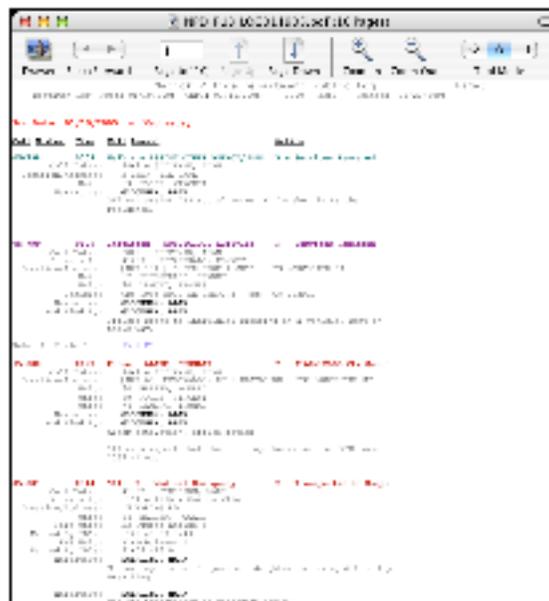
Thanks, Anonymous!

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

Police Reports

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

Police Reports...



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

Sensitive Government Documents

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



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

BLACKHAT BRIEFINGS

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!

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!

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 of ihackstuff.com: murfie, Jimmy Neutron, ThePsyko, Wasabi, Dom, Stonersavant
- Thanks to Roelof T for the great code, and to the current Google blasters: murfie, jimmyneutron, klouw, Dom, stonersavant, MILKMAN, ThePsyko, cybercide, yeseins, wolveso, Deadlink, crash_monkey, zero25, digital.revolution, Renegade334, wasabi, urban, sfd, mlynch, Peefy, Vjxsta, noAcces, brasileiro, john, ZlnCh

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