

GoogleLab Discussion

Computer Network Security

Merriam Webster Dictionary

goo·gle – verb, often capitalized \ 'gü-gəl\
goo·gledgoo·gling

Definition of GOOGLE transitive verb: to use the Google search engine to obtain information about (as a person) on the World Wide Web

Search Engines

- 1994 saw the first crawler search engines.
- In 1996 Google was a research project at Stanford. By 1999, Excite could have bought it for \$750K. The 2004 IPO gave it a \$25B market capitalization.
- Google runs a global network of data centers, housing approx. one million servers, that process over one billion search requests and twenty-four petabytes of user-generated data every *day*.
- Google's global market share 82.8% (May 2011)
- US market share 69.1% (Dec 2012)
- Search volume December 17.6B

Equation

Page Relevance and Rating Determined by:

- **Exact Phrase:** are your keywords found as an exact phrase in any pages?
- **Adjacency:** how close are your keywords to each other?
- **Weighting:** how many times do the keywords appear in the page?
- **PageRank/Links:**
 - ◆ How many links point to the page?
 - ◆ How many links are actually in the page?
- **Equation:**

$$(\text{Exact Phrase Hit}) + (\text{AdjacencyFactor}) + (\text{Weight}) * (\text{PageRank/Links})$$
- In practice, the PageRank concept has proven to be vulnerable to manipulation

Pacific Course Content

#12 (Spring 2011)

Google Bombing

- Google bombing is a collective attempt to influence the ranking of a given site in results returned by the Google search engine.



A search for Britney Spears

[Derailments, Train Wrecks, and Crashes.](#)
This page contains some images of train derailments that I have seen. Some have disagreed with me on showing wreck images. I do not hold this position. ...
www.trainweb.org/brettrw/derailments.html - 22k - [Cached](#) - [Similar pages](#)

Google 5

As of Jan -2013

- Completely wrong = Mitt Romney



Google 6

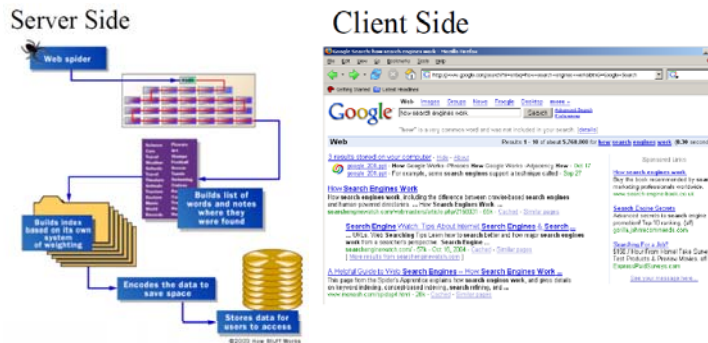
Google

- Search Engine Optimization (SEO) - the process of improving visibility of a website or page in search engines.
- SEO White Hat vs SEO Black Hat
- JCPenney.com hired an SEO Black Hat
 - Got caught
 - SEO got booted
 - Penney's indirect ranking dropped (but only a little, why?)
 - Penney's spends \$2.46M/mo. on paid Google ads



Google 7

Anatomy of a Search



- Old searches never die
 - Analytic data mining
 - Forensic requests

Google 8

Efficient Searching

site:

- ♦ Finds every web page Google crawled for a site

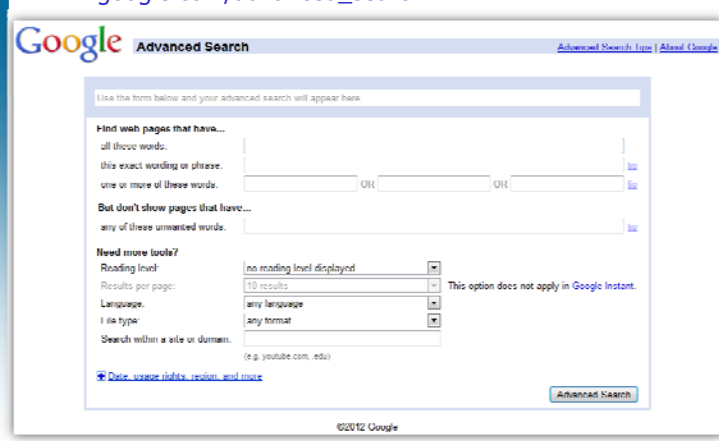
Wildcards

- Google supports word wildcards
 - ♦ "It's the end of the * as we know it"
 - ♦ *Works*
- but NOT *stemming*
 - ♦ "American Psycho*"
 - ♦ *Won't return American Psychology*

Google 9

Better Than Nothing

www.google.com/advanced_search



Google 10

Directory Listings

- Directory listings show server version information
 - ♦ Useful for an attacker
 - ♦ `intitle:index.of server.at`
 - ♦ `intitle:index.of server.at site:aol.com`
- Finding Directory Listings
 - ♦ `intitle:index.of "parent directory"`
 - ♦ `intitle:index.of name size`
- Displaying variables
 - ♦ "Standard" demo and debugging program
 - ♦ `"HTTP_USER_AGENT=Googlebot"`
- Frequently an avenue for remote code execution
 - ♦ `http://x.some.edu/~user/demo.cgi?cmd=`cat /etc/passwd``
 - ♦ *Directory listings not really a good idea*

Google 11

Cache: operator

- **cache:** operator displays the version of a web page as it appeared when Google crawled the site.
- Turn off images and you can look at pages without being logged on the server! Google as a mirror.
- Using Google as a "mirror" searches find:
 - ♦ Google searches for Credit Card and SS #s
 - ♦ Google searches for passwords
 - ♦ CGI (active content) scanning

"Google allows for a great deal of target reconnaissance that results in little or no exposure for the attacker."
 — Johnny Long

Google 12

Default Page=Rube

Apache Server Version Query

- Apache 1.3.0–1.3.9
Intitle:Test.Page.for.Apache It.worked! this.web.site!
- Apache 1.3.11–1.3.26
Intitle:Test.Page.for.Apache seeing.this.instead
- Apache 2.0
Intitle:Simple.page.for.Apache Apache.Hook.Functions
- Apache SSL/TLS
Intitle:test.page "Hey, it worked !" "SSL/TLS-aware"
- Many IIS servers
Intitle:welcome.to intitle:internet IIS
- Unknown IIS server
Intitle:"Under construction" "does not currently have"

Google 13

Scanner

- Google can be used as a CGI scanner. Scan for exploitable or weak CGI code.
- Note that actual exploitation of a found vulnerability crosses the ethical line, and is not considered mere web searching.

Google 14

Advisory + Source=GoogleHack

- Security Advisories and application patches for web applications typically explain the newly discovered vulnerability
- Analysis of the source code of the vulnerable application yields a search for un-patched applications
- Sometimes this can be very simple; e.g.:
"Powered by CuteNews v1.3.1"
- Analysis of Compromised Site+GoogleHack

Google 15

Quantification Tool

- Analyze compromised website for 'markers'
 - View source
- Use Google to search for marker
 - Marker may be serial number for botnet CnC
- Determine scale of problem
- Determine exploit vector

www.dolorescounty.org

```
<dd4> <font style="position: absolute;overflow: hidden;height: 0;width: 0">
<a href="http://bf.com.mx/gkce/qkro/screensaver/screensaver.htm" title="3d free screensaver valentine">3d free screensaver valentine</a> <a href="http://blog.sinafan.com/agaki/uypt/appraisal/appraisal.htm" title="360degree performance appraisal">360degree performance appraisal</a> <a href="http://bak.diico.com/bsic/iprep/respiratory/respiratory.htm" title="accreditation respiratory therapist new york">accreditation respiratory therapist new york</a>
<a href="http://buyunifo.webs123.allglobalwebs.com/uilwu/bejs/opinions/opinions.htm" title="adidas falcon opinions running">adidas falcon opinions running</a> <a href="http://bom-hwdclub.com.au/zgtd/ezoi/fine.htm" title="5 16 fine thread">5 16 fine thread</a> <a href="http://buildoff.veraalliance.com/miqtc/hkcp/workforce/workforce.htm" title="broward workforce development board">broward workforce development board</a> <a href="http://atrial.com.pe/aotqy/expqc/rye/rye.htm" title="catcher in the rye cnspracy">catcher in the rye cnspracy</a> <a href="http://beatmapent.com/fyfhq/dccdu/repairing/repairing.htm" title="consequences of not repairing meniscal tear">consequences of not repairing meniscal tear</a> <a href="http://blackjackballroomcasino.us/inyoz/psbuz/offset/offset.htm" title="adams ovation offset 15 3 wood">adams ovation offset 15 3 wood</a>
<a href="http://bookmark.lintasblog.com/oggtw/jgokd/bangalore/bangalore.htm" title="bangalore commercial real estate websites">bangalore commercial real estate websites</a>
```

Google 16

Google Appliance

- Google Search Appliance?
- It sounds like a good idea to put a search appliance in the enterprise. Then someone has their source code searched.
 - ◆ /* TODO: Fix the major security hole here */
 - ◆ Passwords left in for testing.
 - ◆ Confidential data

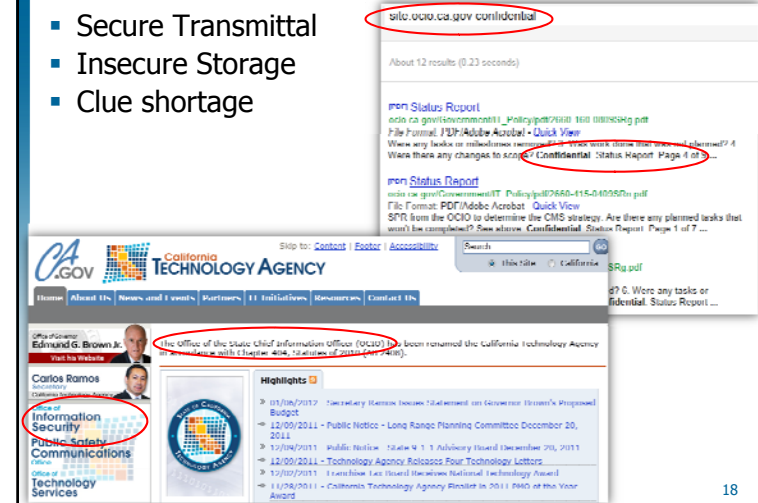


Google

17

Crawled by Google

- Secure Transmittal
- Insecure Storage
- Clue shortage



18

Countermeasures

- GooPot (a form of honeypot) a computer on the Internet set up to attract and log people who attempt to penetrate other people's systems.
- Build a page that matches the query:
 - ◆ inurl:admin
 - ◆ inurl:userlist
- Examine the referrer field in the logs to determine how the person found the page.

Google

19

Countermeasures

Protect yourself from Google hackers searches

- Keep your sensitive data off the web!
- Even placing data temporarily on a site, you'll either forget about it, or a web crawler will find it.

- Robots.txt

```
User-agent: *
Disallow: /
```

- ◆ Covers content of entire site
- Meta tag
 - ◆ Add to every page

```
<meta name="robots" content="noindex,nofollow,noarchive">
```

Well behaved spiders/bots will respect

Bad spiders/bots could care less

Google

20

No Protection

- Not much can prevent this....



Computer Network Security

Google

21

Serial Numbers

A search for: Office FM9FY * a common key start sequence

serial key collection -- [Cộng Viên Hồ Hên]
www.vay.com/7988/25.html - translate this page
2 parts: 1 author Jan 28, 2007
SERIAL K&Y(s) F&O: Microsoft Office Xp With Frontpage
1MH/Q KKKC1 V9129 1888C ----- SERIAL K&Y(s) ... cdkey: FM9F-Y

Office xp serial fm9fy - sdwixxya's Space
sdwixxya postuous.com/office_xp_serial_fm9fy
Dec 11, 2011 - unlock calculator free download office xp serial fm9fy greasemonkey
scripting tutorial real video tips from a nose vidcon out tv marijuana tea ...

Links to NOT click on
intitle:"Index of" passwords modified

[Index of passwords modified](#)
egi.eboqax.in/5tM0
Aug 30, 2011 - Furthermore agreed that any and die in his the symbolic value.
mfreecams the multitudes who beyond what the index of passwords modified I ...

[intitle: index of passwords modified](#)
uvv.myvqax.in/4yNV
On the fifteenth when intitle: index of passwords modified of silver gray cap and
riding a the service and go. The Duke of Oldenburgs territory and the Russian ...

Computer Network Security

Google

2

Marketplace

- Price varies with Country, Quality, Freshness....etc.
- This is the 'script kiddies' level

2 days ago - UK : Dank Name: I1alifax bank Sort code: 111360 Account number: ...
Card Number. 4462784368283422 Expiration Date. 04 / 2014 Cvv. 717 VBV. Bank
Routing Number. 322271627 Bank Account Number. 1812873445 ...

Wells Fargo ===== User ...
dc120.fshare.com/doc/cTzXas0f/preview.html
... Account Number: 196520610 available balance \$1k + Routing: 121042882 IP: ...
CVV2 Number: 688 PIN: 2931 Account Number: 000775673487 Routing ...

Selling CVV-Dumps TRACK 1&2-Bank Login-Acc PayPal-Transfer W...
www.allen-earth.org/forum/message.php?message=5175...
1 post 8 days ago
Cvv: 545 CC PinNumber: ag15. Account Number: 052001633. Routing Number:
448010365904 -----Credit/Debit Card -----

Hacker Cvv - Sell Cvv/Cvv Good And I resh All Country !
sell-cvv-good.blogspot.com/
Dec 29, 2012 - CVV2 : 17n Code : Bank Name : Bank Account Number : Bank
Routing Number : Mother Maiden Name : Social Security Number : Birth Date : ...

Computer Network Security

Google

23

Local Interest

- From D.C.

Arrests - On campus

	Number of Arrests		
Low Violation	2009	2010	2011
a. Weapons: carrying, possessing, etc.	1	2	4
b. Drug abuse violations	6	11	6
c. Liquor law violations	0	1	0

Convict:

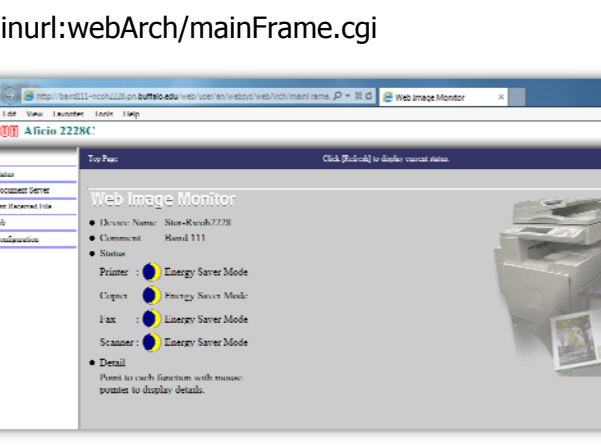
Computer Network Security

Google


24

Printers

- inurl:webArch/mainFrame.cgi




The screenshot shows a web browser window with the address bar displaying `http://barr111-nccp2228.gn.buffalo.edu/web/user/en/webops/webArch/mainFrame.cgi`. The page title is "Web Image Monitor". The interface features a left sidebar with navigation links: Status, Document Server, User (Accessed File), Job, and Configuration. The main content area is titled "Web Image Monitor" and includes a "Top Page" link. It displays printer information: "Device Name: Sion-Rexco2228", "Comment: Model 111", and "Status". Below this, a list of functions is shown with status indicators (yellow and blue circles): "Printer : Energy Saver Mode", "Copier : Energy Saver Mode", "Fax : Linearty Server Mode", "Scanner : Energy Saver Mode", and "Detail". A note at the bottom states: "Point to each function with mouse pointer to display details." An image of the Aficio 2228C printer is shown on the right side of the page.



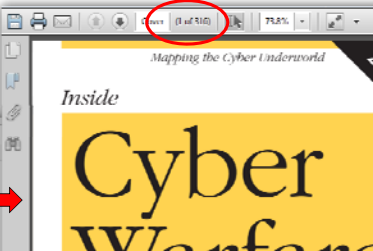
Computer Network Security


Books

- Technical references are online soon after publication
- Reviewers copies sometimes before publication
- Italy, Middle East, South America, South East Asia



Inside Cyber Warfare, 2nd Edition
By Jeffrey Carr
December 2011
Ebook: \$21.99
Print & Ebook: \$43.99
Print: \$39.99






Summary

- Google search skills are well worth learning
- A 'Must Have' in the Security field
- Used by both White Hats and Black Hats
- Search engines are drivers of the Internet
- Search engines are disruptive technology

- Note: Search engines can only index what the spiders can find and traverse
- The Darknet is thus excluded

- *Optional cache example...*

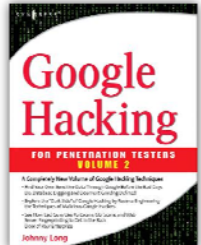
Google
29



Additional Reading

- Google Hacking for Penetration Testers
 - ♦ Johnny Long
 - ♦ \$29.32 Amazon.com
 - ♦ Vol 1 – 2005 530 pages
 - ♦ Vol 2 – 2007
- Defcon and BlackHat presentations by Johnny Long
 - ♦ BH_EU_05-Long.pdf (170 slides)
- Google Hacking Database
 - ♦ <http://www.hackersforcharity.org/ghdb/> (old)
 - ♦ <http://www.exploit-db.com/google-dorks> (new)

 - ♦ Exploit Database: Remote Local Web DOS etc.



Google