Objective

Google Hacking refers to the technique of using Google Search to find security holes in the configuration and code that websites use. Searches can reveal sensitive information, such as username/passwords, internal documents, etc. The techniques are commonly used during penetration testing. Google Hacking is based on using structured searches with advanced operators to quickly and accurately obtain results. This is a skill-set development lab to enhance your Google-fu. Put in 60 minutes or more working on your search skills. Try some of the searches provided.

Caveats

- Look but don’t exploit
- Activity shows up in web logs and some IPS tools
- Watch out for Honeypots, SEO poisoning, and Traps

Look and Think before you click
Requirements

- The network security lab is isolated from the campus, this assignment requires a computer with Internet access. If you use your computer, make sure it is fully patched (OS, BHO, Adobe, Players, etc) and the firewall is on.

To get started

- Open any internet browser
- Type www.google.com into the address bar

Be specific:

- + for exact word match
- - to exclude word
- """" for exact phrase match
- Use 100 results per page
Google Search Operators

- **link: url** shows other pages with links to that url
- **related: url** same as "what's related"
- **site: domain** restricts search results to the given domain
- **allinurl:** shows only pages with all terms in the url
- **inurl:** like allinurl, but only for the next query word
- **allintitle:** shows only results with terms in title
- **intitle:** like allintitle, but only for the next word
- **cache: url** shows the version from Google's cache
- **info: url** shows links to related searches, pages containing url
- **filetype:** searches for that filetype, -filetype excludes that type
- **daterange:** supported in Julian date format only
- **maps:** enter a street address
- **phonebook:** shows all public phonebooks
- **allintext:** searches only within text of pages
- **allinlinks:** searches only within links, not text or title

This is not a complete listing, a space after the : may/may not be needed
The **site:** operator

The **site:** search is invaluable in all directed Google searches. Combined with a host or domain name, the results are listed in page-ranked order. Type **site:pacific.edu** into the Google search bar.
Further refining the search:

- After *site: pacific.edu*, type in *login / logon* and run the search.

*login / logon* finds login pages associated with any particular website – the significance of this is that login pages are the “front door” and often reveal the nature of the operating system, software, and even offer clues for gaining access to the site.

- The results show the main login page associated with Pacific (insidePacific), as well as student and staff logins.
Several variations of basic Google searches like the `login` | `logon` are:

- `username` | `userid` | `employee.ID` | “your username is”
- `admin` | `administrator`
- `password` | “your password is”
- `error` | `warning`

These queries are good for checking servers to locate possible vulnerabilities and determining what software is being used. This allows attackers with a particular exploit to locate potential targets.

Sometimes, viewing the source of the page, will turn up this:

```bash
# host system constants:
MY_USER = 'apache'
PASSWD = 'apa4che8'
RSYNC_BIN = '/usr/local/bin/rsync'
PATH_TO_FTP_LOG = '/var/log/vsftpd.log'
SSH_BIN = '/usr/bin/ssh'
```
inurl:temp | inurl:tmp | inurl:backup | inurl:bak
The **inurl** prefix will cause Google to find any file that contains what was specified. **inurl:** can be used with any other search term.

**intitle:**
The **intitle** prefix will cause Google to search for any terms within the title (the html `<title>` tag) of the document. As with **inurl**, **intitle** can be used with other search terms.

**intitle:index.of.config** – These directories can give information about a web servers configuration, such as ports, security permissions, etc.

**intitle:index.of.etc** – The `/etc/` directory often contains password files which are usually protected with an md5 hash.
Examples of other uses of intitle:

- **intitle:index.of mp3 jackson** – Brings up listings of files and directories that contain “mp3” and “jackson.”

Warning: malware sites may spoof intitle content.

- **intitle:index.of passwd passwd.bak** – similar for password files

- **intitle:error/ intitle:warning** – Finds error, warning pages, often revealing server version numbers

### Results of the **intitle:index.of mp3 jackson** search
Special operators in searches

While creating searches that look for exploits, there are several special operators that Google recognizes that are sometimes necessary for the desired results.

- (""") – Surrounding a search term in quotes causes Google to include all the terms specified, in the order they are specified.
- (-) – Use before an operator to exclude the search term following it. (i.e. -ext:html would exclude all html files from the results)
- (.) – Use to represent a single character wildcard (i.e. -intitle:index.of searches cause the period to recognize a space in between “index” and “of”).
- (*) – Use to represent a single word wildcard (i.e. - "growth demands a * * * *“ returns the quote “Growth demands a temporary surrender of security.”
Other useful searches

**phonebook: <name><city>** - Gives the home phone and often the address of any name you put in.

**ext:(doc | pdf | xls | txt | ps | rtf | odt | sxw | psw | ppt | pps | xml)** - limits Google to displaying only the filetypes specified, which may contain confidential information or other pertinent data not meant for outsiders to see (same as filetype:).

"robots.txt" "disallow:" filetype:txt – searches for the text file “robots,” which specifies to the Google crawler what pages on a particular website the webmaster does not want searchable; using this search returns a list of all those locations.
Google countermeasures to protect the lame

- Searches designed specifically to find credit card numbers (i.e. 300000000000000..399999999999999) or for probing for password/config directories may be “blocked” by Google using either:
  - A page stating it cannot process your request due to its resemblance of a bot search
  - A CAPTCHA prompt which will still allow the search after user input
Below are some searches for servers with network cameras, including traffic, weather, office, and pet-cams. Unsecured cameras allow the camera to be tilted, panned, zoomed, etc. Look for results that use an IP address, beware of malware sites. (Safe Search On)

intitle:"Live View / - AXIS 206W"
WebcamXP - "powered by webcamXP" "Pro|Broadcast"
inurl:axis-cgi/mjpg
inurl:view/indexFrame.shtml
inurl:ViewerFrame?Mode=Refresh
inurl:"viewerframe?/mode=motion"
site:axiscam.net

The content abstract gibberish (and the warning from Google) are clear warnings.
Searches for printers are more useful when ran *inside* a network. The printer below shows an error. Note the ‘Properties’ button. Printers offer hours of potential entertainment (*anyone trying to use the printer may not be as entertained*). Changing printer settings can be a form of DoS.

`intitle:Home "display printer status"`
Examples of different searches:

inurl:ConnectComputer/precheck.htm
inurl:Remote/logon.aspx
intitle:“Welcome to 602LAN SUITE *”
initle:“index of /backup“
“parent directory” DVDRip -xxx -html -php -shtml -opendivx
inurl(company) filetype:iso
"#-FrontPage-" inurl:service.pwd
intitle:"Index of" config.php

The last search can turn up a username/password for a SQL database that is part of a web-based forum application, the prize? admin access

Running the query also turned up…. (see next page)
Insufficient Clue
A search for SSHTerm and SSHVnc applets:
“loading the applet” “you will be asked to accept a certificate registered to 3SP LTD”
More examples of interesting searches:

“Powered by”
“This site is using”
“This site created by”
“This website powered by”
“This script created by”
“Thank you for using”
“Welcome to the”

enable password | secret “current configuration”
intitle:“TOPdesk ApplicationServer”

A search for the TOPdesk default logon found: admin/admin
Even more examples of interesting searches

intitle:“Error Occurred While”
“not for public release” (url:*.edu |*.gov |*.mil)
“not for public release” -.edu -.gov -.mil
“not for distribution” confidential
“internal working draft”
“Thank you for your order” +receipt
"phone * * *" "address *" "e-mail" intitle:"curriculum vitae"
"phpMyAdmin" "running on" inurl:"main.php"
"Network Vulnerability Assessment Report"

filetype:pdf "hacking exposed 6th"
SHOUTcast is cross-platform proprietary software for streaming media over the Internet. The SHOUTcast admin page can be used to kick off users, ban their IP address, or ban their subnet.

intitle:"SHOUTcast Administrator" inurl:admin.cgi

As of 2011, almost 1M concurrent listeners can be seen online, spread across ~50K stations. The streams are TCP, typically 96kbs to 128kbs.
Google Hacking for Cameras

intitle: axis intitle: “video server”
intitle: liveapplet inurl: LvAppl
intitle: “EvoCam” inurl: “webcam.html”
intitle: “Live NetSnap Cam-Server feed”
intitle: “Live View / &amp;#8211; AXIS”
intitle: “Live View / &amp;#8211; AXIS 206M”
intitle: “Live View / &amp;#8211; AXIS 206W”
intitle: “Live View / &amp;#8211; AXIS 210”
inurl: indexFrame.shtml Axis
inurl: “MultiCameraFrame?Mode=Motion”
intitle: start inurl: cgistart
intitle: “WJ-NT104 Main Page”
intext: “MOBOTIX M1” intext: “
intext: “MOBOTIX M10” intext: “
intext: “MOBOTIX D10” intext: “
inurl: snc-z20 inurl: home/
inurl: snc-cs3 inurl: home/
inurl: snc-rz30 inurl: home/
intitle: “sony network camera snc-p1”
intitle: “sony network camera snc-m1”
site: .viewnetcam.com -www.viewnetcam.com

inurl: /view.shtml
inurl: ViewerFrame?Mode=
intitle: “Live View / &amp;#8211; AXIS”
inurl: /view/view.shtml
inurl: ViewerFrame?Mode=Refresh
inurl: axis-cgi/jpg
inurl: axis-cgi/mjpg (motion-JPEG)
inurl: view/indexFrame.shtml
inurl: view/index.shtml
inurl: view/view.shtml
liveapplet
intitle: “live view” intitle: axis
intitle: liveapplet
intitle: “Toshiba Network Camera” user login
intitle: “netcam live image”
intitle: “i-Catcher Console &amp;#8211; Web Monitor”
"Vbrick Integrated Web Server (IWS) Login"

VBrick Security Issue
Over time, many search patterns become less useful as users and vendors become aware (aka: gain clue). New search patterns tend not to be widely shared in order to prolong their useful lifespan (and maybe to increase sales of books on the subject).

Good Google searching skills are part skill - part art!

Additional Links

www.googleguide.com/
www.exploit-db.com/google-dorks/
www.stachliu.com/resources/tools/google-hacking-diggity-project/

“Once upon a time, all the roads led to Rome. Today, all roads lead from Google.” - JeffJ arvis
Homework/Lab Turn-In

- Turn this page in.  Name: ____________________________

- Create a specific search for something, adding search operators to narrow the results. Show the search you used to get the most specific results. _______________________________________

- Google for yourself. Can you find any images of yourself? Any pages that list your address, phone, etc.? Any that you were not aware of? _____________________________________________

- There are at least two ways to keep Google from indexing content. What are they?

- What was the most interesting search you tried, and why?