blackMORE Ops

HACK, **HOW TO**

Useful Google hacks

JULY 8, 2014 | BLACKMORE OPS | LEAVE A COMMENT

I've been searching Internet and found lots of interesting info about how to use Google for pentests and different intuitive ways to use search strings to get useful information. Googledorks already uses these to compile their lists. However I was unable to find some information and explanations in there. So I've decided to compile a nice guide for Useful Google Hacks and Tricks for readers and myself. I've included as much credits I can at the bottom of this post including authors websites, however, if I've missed any, feel free to comment and I'll ensure they are included. Also note that, these information's are publicly available in many websites, so it was quite hard for me to credit original authors/finders.

Useful Google Hacks

Google is #1 ranked search engine in modern internet. They are a giant who got access to your website, your mobile, your eCommerce site, your IRC site and god knows what else. That means they get a massive amount of information's and data. Out of those there's always the chance of leaked sensitive data such as server config, password file, backup file, proprietary materials such as eBooks, Music, PDF, Word Documents, Serial Number etc. In this post I will try to show how to use Google pentests to gather information and looks for exploitable information. If you find something important, please try to contact the owner and report the search string to Google rather than abusing it. I am not responsible how readers might or mights not use the information provided below. Read my Disclaimer (http://www.blackmoreops.com/about/disclaimer/)and Privacy Policy (http://www.blackmoreops.com/about/privacy-policy/).

(https://blackmoreops.files.wordpress.com/2014/07/useful-google-hacks.jpg)

Pentesting Security Cameras

Now this is a known one, We've all tried it at some point. I am not even sure if this is allowed or not, but I definitely think IP cameras should be more secured so that people can't look into your Baby Monitor or simple Home Security Cameras. Different vendors provided product specific patches in different times, be sure to spread the word so that you're not the victim of unsolicited prying.

There exists many security cameras used for monitoring places like parking lots, college campus, road traffic etc. which can be pentested using Google so that you can view the images captured by those cameras in real time. All you have to do is use the following search query in Google. Type in Google search box exactly as follows and hit enter

```
inurl:"viewerframe?mode=motion"
```

Click on any of the search results (Top 5 recommended) and you will gain access to the live camera

which has full controls.

You now have access to the Live cameras which work in real-time. You can also move the cameras in all the four directions, perform actions such as zoom in and zoom out. This camera has really a less refresh rate. But there are other search queries through which you can gain access to other cameras which have faster refresh rates. So to access them just use the following search query.

```
intitle:"Live View / – AXIS"
```

Click on any of the search results to access a different set of live cameras. Thus you have pentested Security Cameras using Google.

Pentesting Personal and Confidential Documents

Using Google it is possible to gain access to an email repository containing CV of hundreds of people which were created when applying for their jobs. The documents containing their Address, Phone, DOB, Education, Work experience etc. can be found just in seconds.

```
intitle:"curriculum vitae" "phone * * *" "address *" "e-mail"
```

You can gain access to a list of .xls (excel documents) which contain contact details including email addresses of large group of people. To do so type the following search query and hit enter.

```
filetype:xls inurl:"email.xls"
```

Also it's possible to gain access to documents potentially containing information on bank accounts, financial summaries and credit card numbers using the following search query

```
intitle:index.of finances.xls
```

Pentesting Google to gain access to Free Stuffs

Ever wondered how to pentest Google for free music or eBooks. Well here is a way to do that. To download free music just enter the following query on Google search box and hit enter.

```
"?intitle:index.of?mp3 eminem"
```

Now you'll gain access to the whole index of Eminem album where in you can download the songs of your choice. Instead of Eminem you can substitute the name of your favorite album. To search for the eBooks all you have to do is replace "Eminem" with your favorite book name. Also replace "mp3" with "pdf" or "zip" or "rar".

Using specialized search strings in Google

If I remember correctly, recent Google update (from HTTP to HTTPS) and backend modification fixed some of the following issues. However, here goes:

METHOD 1

For Example we can find:
Credit Card Numbers
Passwords
Software / MP3's
…… (and on and on and on) Presented below is just a sample of interesting searches that we can send to Google to obtain info that some people might not want us having.. After you get a taste using some of these, try your own crafted searches to find info that you would be interested in.

Try a few of these searches:

```
intitle:”Index of” passwords modified
allinurl:auth*user*file.txt
“access denied for user” “using password”
“A syntax error has occurred” filetype:ihtml
allinurl: admin mdb
“ORA-00921: unexpected end of SQL command”
inurl:passlist.txt
“Index of /backup”
“Chatologica MetaSearch” “stack tracking:”
Amex Numbers: 300000000000000..399999999999999
MC Numbers: 5178000000000000..5178999999999999
visa 4356000000000000..4356999999999999 (http://www.google.com
/search?q=visa+4356000000000000..4356999999999999&sourceid=firefox&
start=0&start=0&ie=utf-8&oe=utf-8)
“parent directory ” /appz/ -xxx -html -htm -php -shtml -opendivx -md5
-md5sums
“parent directory ” DVDRip -xxx -html -htm -php -shtml -opendivx -md5
-md5sums
“parent directory “Xvid -xxx -html -htm -php -shtml -opendivx -md5
-md5sums
“parent directory ” Gamez -xxx -html -htm -php -shtml -opendivx -md5
-md5sums
“parent directory ” MP3 -xxx -html -htm -php -shtml -opendivx -md5
-md5sums
“parent directory ” Name of Singer or album -xxx -html -htm -php -shtml
-opendivx -md5 -md5sums
```

Notice that I am only changing the word after the parent directory, change it to what you want and you will get a lot of stuff.

METHOD 2

Put this string in Google search:

```
?intitle:index.of? mp3 (http://www.google.com/search?hl=en&lr=&ie=UTF-
8&c2coff=1&q=Example%3A+%3Fintitle%3Aindex.of%3F+mp3+jackson)
```

You only need add the name of the song/artist/singer.

```
Example: ?intitle:index.of? mp3 jackson
```

METHOD 3

Put this string in Google search:

```
inurl:microsoft filetype:iso (http://www.google.com/search?hl=en&
lr=&ie=UTF-8&c2coff=1&q=inurl%3Amicrosoft+filetype%3Aiso)
```

You can change the string to whatever you want, ex. Microsoft to adobe, ISO to zip etc…

```
“# -FrontPage-” inurl:service.pwd (http://www.google.com/search?hl=en&
lr=&ie=UTF-8&c2coff=1&q=%22%23+-FrontPage-%22+inurl%3Aservice.pwd)
```

FrontPage passwords.. very nice clean search results listing !!

```
 “AutoCreate=TRUE password=”  (http://www.google.com/search?hl=en&
lr=&ie=UTF-8&c2coff=1&q=%22AutoCreate%3DTRUE+password%3D*%22+)
```

This searches the password for “Website Access Analyzer”.

```
“http:// (http://www.google.com/search?hl=en&lr=&ie=UTF-8&c2coff=1&
q=%22http%3A%2F%2F*%3A*@www%22+domainname):@www” domainname
(http://www.google.com/search?hl=en&lr=&ie=UTF-8&c2coff=1&q=%22http%3A%2F
%2F*%3A*@www%22+domainname)
```

This is a query to get inline passwords from search engines (not just Google), you must type in the query followed with the the domain name without the .com or .net

```
“http:// (http://www.google.com/search?hl=en&lr=&ie=UTF-8&c2coff=1&
q=%22http%3A%2F%2F*%3A*@www%22+bangbus):@www” bangbus
(http://www.google.com/search?hl=en&lr=&ie=UTF-8&c2coff=1&q=%22http%3A%2F
%2F*%3A*@www%22+bangbus) or “http:// (http://www.google.com/search?hl=en&
lr=&ie=UTF-8&c2coff=1&q=%22http%3A%2F
%2F*%3A*@www%22bangbus):*@www”bangbus (http://www.google.com/search?hl=en&
lr=&ie=UTF-8&c2coff=1&q=%22http%3A%2F%2F*%3A*@www%22bangbus)
```

Another way is by just typing

```
 “http://bob:bob@www” (http://www.google.com/search?hl=en&lr=&ie=UTF-
8&c2coff=1&q=%22http%3A%2F%2Fbob%3Abob@www%22)
```

```
"sets mode: +k" (http://www.google.com/search?hl=en&lr=&ie=UTF-8&c2coff=1&
q=%22sets+mode%3A+%2Bk%22)
```

This search reveals channel keys (passwords) on IRC as revealed from IRC chat logs.

```
 allinurl: admin mdb (http://www.google.com/search?hl=en&lr=&ie=UTF-
8&c2coff=1&q=allinurl%3A+admin+mdb)
```

Not all of these pages are administrator's access databases containing usernames, passwords and other sensitive information, but many are!

```
allinurl:auth*user*file.txt (http://www.google.com/search?hl=en&lr=&ie=UTF-
8&c2coff=1&q=allinurl%3Aauth_user_file.txt)
```

DC Forum's password file. This file gives a list of (crackable) passwords, usernames and email addresses for DC Forum and for DCShop (a shopping cart program(!!!). Some lists are bigger than others, all are fun, and all belong to Googledorks. =)

```
intitle:"Index of" config.php (http://www.google.com/search?hl=en&
lr=&ie=UTF-8&c2coff=1&q=intitle%3A%22Index+of%22+config.php)
```

This search brings up sites with **"config.php"** files. To skip the technical discussion, this configuration file contains both a username and a password for an SQL database. Most sites with forums run a PHP message base. This file gives you the keys to that forum, including FULL ADMIN access to the database.

```
eggdrop filetype:user user (http://www.google.com/search?hl=en&lr=&ie=UTF-
8&c2coff=1&q=eggdrop+filetype%3Auser+user)
```

These are eggdrop config files. Avoiding a full-blown discussion about eggdrops and IRC bots, suffice it to say that this file contains usernames and passwords for IRC users.

```
intitle:index.of.etc (http://www.google.com/search?hl=en&lr=&ie=UTF-
8&c2coff=1&q=intitle%3Aindex.of.etc)
```

This search gets you access to the etc directory, where many many many types of password files can be found. This link is not as reliable, but crawling etc directories can be really fun!

```
filetype:bak inurl:"htaccess|passwd|shadow|htusers" (http://www.google.com
/search?hl=en&lr=&ie=UTF-8&c2coff=1&q=filetype%3Abak+inurl
%3A%22htaccess%7Cpasswd%7Cshadow%7Chtusers%22)
```

This will search for backup files (*.bak) created by some editors or even by the administrator himself (before activating a new version). Every attacker knows that changing the extension of a file on a Web server can have ugly consequences.

Let's pretend you need a serial number for Windows XP Pro.

In the Google search bar type in just like this –

```
"Windows XP Professional" 94FBR (http://www.google.com/search?hl=en&
lr=&ie=UTF-8&c2coff=1&q=%22Windows+XP+Professional%22+94FBR)
```

the key is the **94FBR** code.. it was included with many MS Office registration codes so this will help you dramatically reduce the amount of 'fake' porn sites that trick you.

or if you want to find the serial for Winzip 8.1 – **"Winzip 8.1" 94FBR**

If you managed to find something useful using these search methods, I suggest you try out this guide:

How to pentest Remote PC (Windows 2003 server) with Metasploits (http://www.blackmoreops.com/2013/11/02/how-to-pentest-remote-pc-windows-2003-server-with-metasploits/)

Metasploit is a powerful took which helps users to pentest their system. It's easy to use and it's informative at the same time.

Using special search string to find vulnerable websites

Following search strings in Google will come up with bunch of results. You can try one at a time and run SQLmap to pentest a vulnerable website

```
inurl:php?=id1
inurl:index.php?id=
inurl:trainers.php?id=
inurl:buy.php?category=
inurl:article.php?ID=
inurl:play_old.php?id=
inurl:declaration_more.php?decl_id=
inurl:pageid=
inurl:games.php?id=
inurl:page.php?file=
inurl:newsDetail.php?id=
inurl:gallery.php?id=
inurl:article.php?id=
inurl:show.php?id=
inurl:staff_id=
inurl:newsitem.php?num= andinurl:index.php?id=
inurl:trainers.php?id=
inurl:buy.php?category=
inurl:article.php?ID=
inurl:play_old.php?id=
inurl:declaration_more.php?decl_id=
inurl:pageid=
inurl:games.php?id=
inurl:page.php?file=
inurl:newsDetail.php?id=
inurl:gallery.php?id=
inurl:article.php?id=
inurl:show.php?id=
inurl:staff_id=
inurl:newsitem.php?num=
```

I have shown you this info to let you know that there is a real risk putting your info online. If you do want to buy stuff online make sure the site you are using is secure normally if a site is secure you will see a pop up saying you are now entering a secure part of the site or a symbol of a padlock at the bottom of your browser or just use pay pal, pay pal is very safe to use. But most of the time just use common sense if a site looks cheap it normally hasn't got the protection to keep your info safe. I am not saying don't buy stuff online because that is one of the best thing's about the internet i am just saying be aware of websites that want your bank details and there is no symbol of a padlock at the bottom of your browser.

Thanks for reading. Please share.

Sources and Credits as due:

1. http://johnny.ipenteststuff.com/ (http://johnny.ipenteststuff.com/)
2. http://www.i-pentested.com/ (http://www.i-pentested.com/)
3. http://www.aagneyam.com/ (http://www.aagneyam.com/)

HACKING **HOW TO**

Follow

Follow “blackMORE Ops”