Google Dorking for a More (in)Secure Internet

Hello!

I am Jonathan “Doc Panda” Briggs

I am here because I love to give presentations.

I am the founder of Defcon Group 559.

You can find me at @PandaPhDminus

Disclaimer

I am not responsible for whatever you may do with the information located within this talk. This is for educational purposes only.

Please contact your lawyer, doctor, professor, pharmacist, grocer, YouTuber, farmer, BFF, or SPCA before attempting any of this.

1

What is Google Dorking?

> “Google hacking, also named Google dorking, is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use.
>
> -Wikipedia

Why do we need Google Dorking?

FOR PENETRATION TESTING:

It provides an attack vector in which passwords, social engineering info, or corporate details can be leaking out to the world.

This could be providing information for a future breach with little to no fingerprint for the attacker.

FOR SECURITY:

Finding any possible attack vectors can be patched and removed before found by malicious actors.

Whether attacking or defending your network and data, Google Dorking is a good open-source tool to use to check what may or may not be public.

2

How do I dork Google?

Google Search Basics

- Search queries are not case-sensitive
- 32 word search limit
- Wildcard (*)
- Boolean Operators (+ - |)
- Quotes

Syntax

operator:search_term

No spaces between the operator, colon, and search term.

Operators beginning with the word ALL can be used once per search and not mixed with other operators.

Boolean operators can be used as long as they do not interfere with the separating colon.

Example: *intitle:Login inurl:login.php intext:admin/admin*

intitle and allintitle

Intitle uses the word after the colon as a title search, and the other words past that word as extra search parameters, not necessarily in title.

Allintitle uses all the words after the colon as a title search.

The title of a page can be the text at the top of a webpage, or found in the HTML TITLE tag.

inurl and allinurl

Inurl searches for the word in a site's pathname.

Allinurl searches for several words or phrase in a site's pathname.

Note 1: It may be easier to use multiple instances of inurl, rather than using allinurl.

Note 2: Google can't effective search the protocol section of the URL (http, ftp, etc.).

site and filetype

site reduces a search to only the domain specified.
Example: *Google dorking site:valleydevfest.com*

filetype searches for files of a specified type.

Example: *filetype:xls payroll*

cache

cache searches for a cached version of a website. It must be used with a domain name, else it will be used as a regular search, searching your term and the word cache.

Example: *cache:google.com*

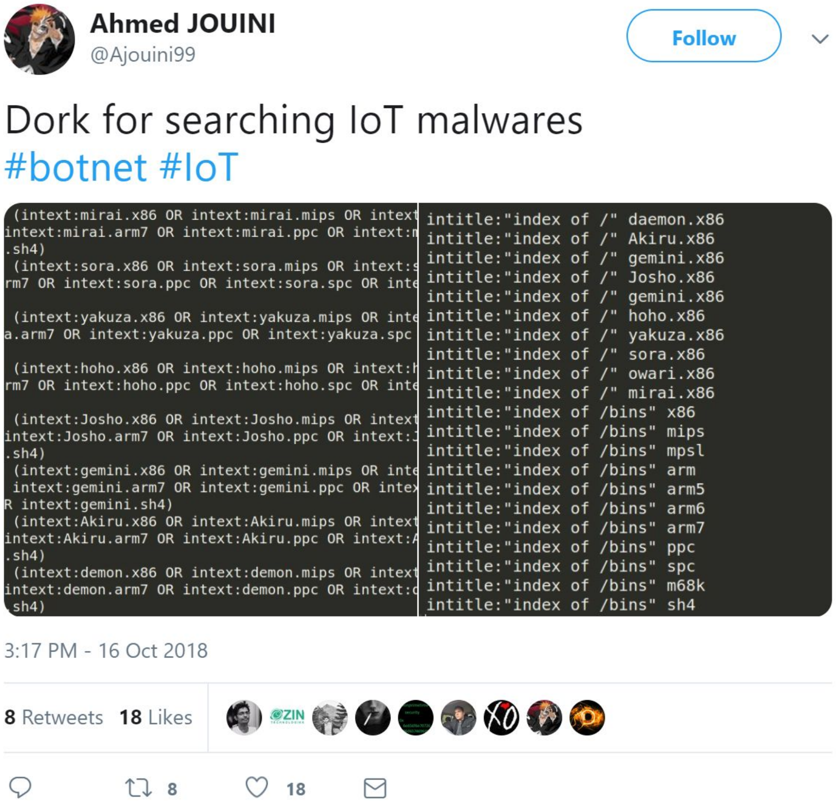
related

related finds pages related to the webpage you are searching. Using a search term that is not a domain will result in a regular search.

Example: *related:gdgfresno.com*

Real-World Example

https://twitter.com/Ajouini99/status/1052322638855622656



Ahmed JOUINI
@Ajouini99

Dork for searching IoT malwares #botnet #IoT

```
 (intext:mirai.x86 OR intext:mirai.mips OR intext
intext:mirai.arm7 OR intext:mirai.ppc OR intext:m
.sh4)
 (intext:sora.x86 OR intext:sora.mips OR intext:s
rm7 OR intext:sora.ppc OR intext:sora.spc OR inte

 (intext:yakuza.x86 OR intext:yakuza.mips OR inte
a.arm7 OR intext:yakuza.ppc OR intext:yakuza.spc

 (intext:hoho.x86 OR intext:hoho.mips OR intext:h
rm7 OR intext:hoho.ppc OR intext:hoho.spc OR inte

 (intext:Josho.x86 OR intext:Josho.mips OR intext
intext:Josho.arm7 OR intext:Josho.ppc OR intext:J
.sh4)
 (intext:gemini.x86 OR intext:gemini.mips OR inte
 intext:gemini.arm7 OR intext:gemini.ppc OR intex
R intext:gemini.sh4)
 (intext:Akiru.x86 OR intext:Akiru.mips OR intext
intext:Akiru.arm7 OR intext:Akiru.ppc OR intext:A
.sh4)
 (intext:demon.x86 OR intext:demon.mips OR intext
intext:demon.arm7 OR intext:demon.ppc OR intext:d
 sh4)
```

```
intitle:"index of /" daemon.x86
intitle:"index of /" Akiru.x86
intitle:"index of /" gemini.x86
intitle:"index of /" Josho.x86
intitle:"index of /" gemini.x86
intitle:"index of /" hoho.x86
intitle:"index of /" yakuza.x86
intitle:"index of /" sora.x86
intitle:"index of /" owari.x86
intitle:"index of /" mirai.x86
intitle:"index of /bins" x86
intitle:"index of /bins" mips
intitle:"index of /bins" mpsl
intitle:"index of /bins" arm
intitle:"index of /bins" arm5
intitle:"index of /bins" arm6
intitle:"index of /bins" arm7
intitle:"index of /bins" ppc
intitle:"index of /bins" spc
intitle:"index of /bins" m68k
intitle:"index of /bins" sh4
```

3:17 PM - 16 Oct 2018

8 Retweets 18 Likes

3

Simple Security Searches

Getting good results to start.

site

Site can be used to gather information on hosted and maintained servers.

Example: site:bitwiseindustries.com -site:www.bitwiseindustries.com

intitle:index.of, intitle:“index of”

Displays directory listings. Very useful for finding information.

Example: intitle:index.of backup

error OR warning

Appropriately used, can be used to find server information or information about logins and passwords.

Example: (“for more information”) (error | warning)

login OR logon

Helpful for finding login portals for websites.

Example: site:gdgfresno.com login|logon

admin OR administrator

Can help locate administration pages, or find information on administrators.

Example: admin | administrator site:valleydevfest.com

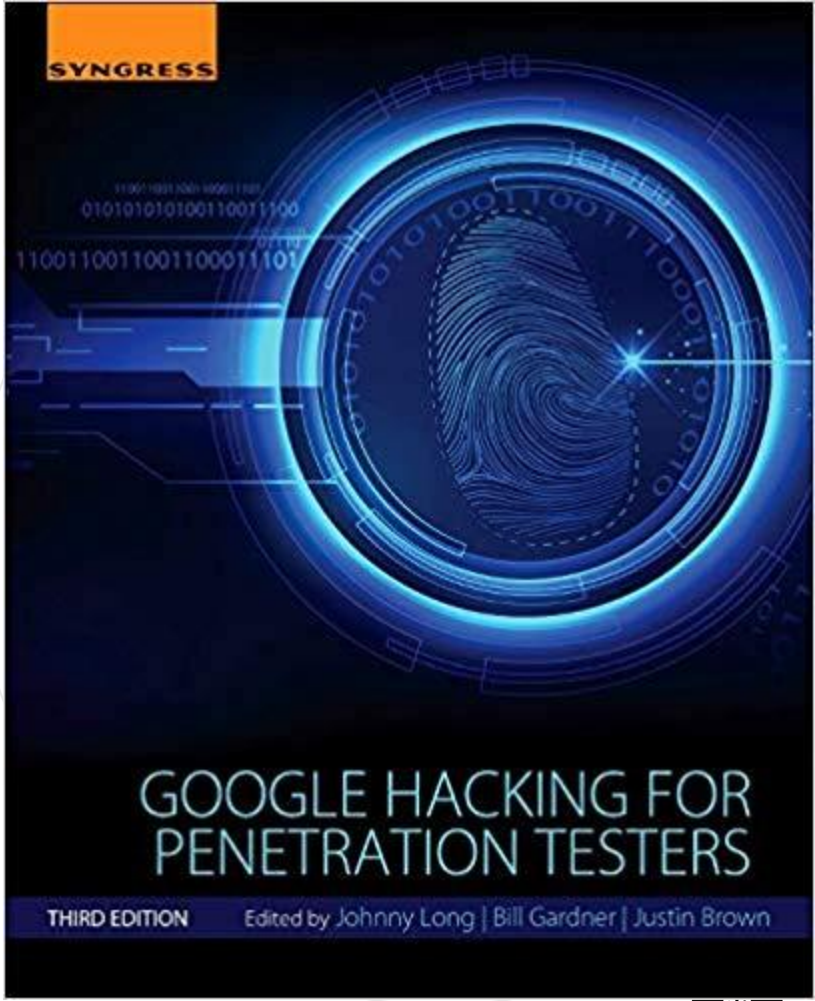
4

More Information

Where do I go from here?

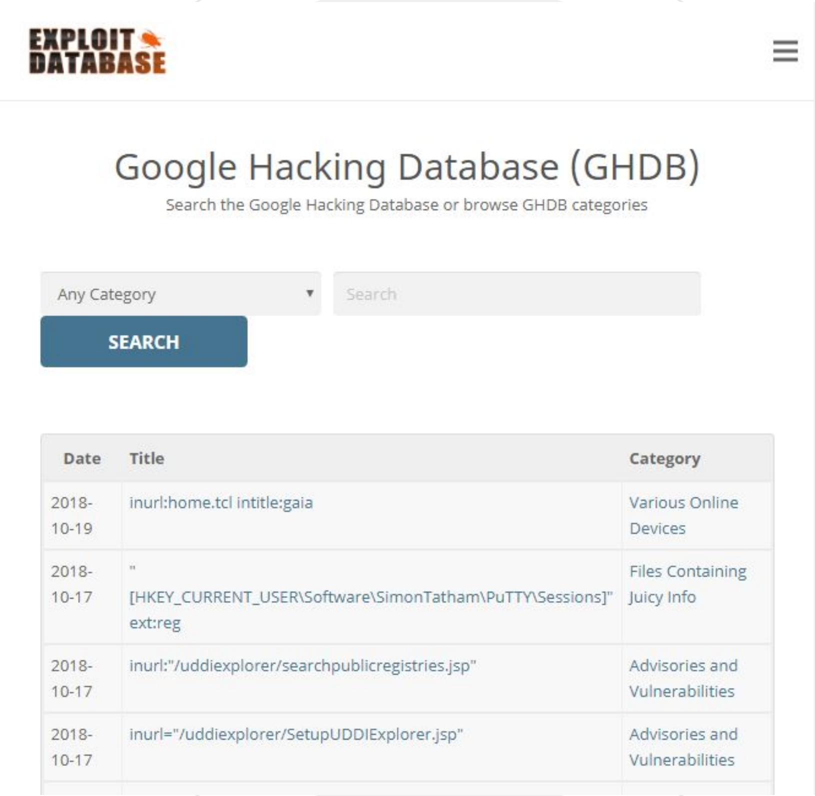
Google Hacking for Penetration Testers, Third Edition

The book on Google Dorking. In its third edition, it has been the definition of all things Google Hacking.


SYNGRESS
GOOGLE HACKING FOR PENETRATION TESTERS
THIRD EDITION
Edited by Johnny Long | Bill Gardner | Justin Brown

Google Hacking Database

A database, hosted by Offensive Security, that freely shares Google Dorks, and allows for submission by anyone.



Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Date	Title	Category
2018-10-19	inurl:home.tcl intitle:gaia	Various Online Devices
2018-10-17	"[HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions]" ext:reg	Files Containing Juicy Info
2018-10-17	inurl:"/uddiexplorer/searchpublicregistries.jsp"	Advisories and Vulnerabilities
2018-10-17	inurl="/uddiexplorer/SetupUDDIExplorer.jsp"	Advisories and Vulnerabilities

Thanks!

Any questions?

You can find me at

- @PandaPhDminus
- pandaphdminus@gmail.com
- probablymalware.org
- www.linkedin.com/in/jonathan-r-briggs

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash