GOOGLE DORKING TECHNIQUES BY RED TEAMERS

For example in Offensive Security Solutions Google Dorking is crucial to use before the assessment. These techniques are not usually given in professional pentesting either due to a lack of skill or because cheaper options are offered that are not provided. If you would want to know what this could reveal to an attacker, often times you can find publicly available sensitive information for any company or keywords specifically in your country or other factors so that you can use to limit the results to what you are looking for, in a one-liner and that serves as a quick shortcut to sometimes getting credentials, sensitive pdf files or client information.

Let's say you want to search for all publicly available PDF files in a specific country using Google. You can easily provide the following:

```
'nda filetype:pdf location:malta'
```

SWIPE

SIMPLE DORKING EXAMPLES

Here are some examples of using dorking. This is considered OSINT, which means you are using open-source available data using a search engine that has already indexed them.

1) Search for websites that contain the word "crypto" and a number between 1 and 1337:

```
"crypto" 1..1337
```

2) Search for the term "VideoName" but exclude results from YouTube:

```
VideoName -site:youtube.*
```

3) Search for websites published after the 1st January 2023 dealing about how to use ‘/repair/shutdown/... a computer’:

```
How to * a computer after:2023-01-01
```

4) Search for websites published before 2023 which have the TLD .gov, are either html or php documents and contain the words "homework", "teacher" and "school":

```
allintext:homework teacher school site:gov before:2023
ext:(html | php)
```

Now that, is a really powerful one-liner that can get you sensitive information.

COMPLEX DORKING EXAMPLES WITH VALUABLE INFO

- Find open/public webcams available with direct links:

  `intitle:"webcamXP 5" | inurl:"lvappl.htm"`

- Find log documents which have the string "password" in it:

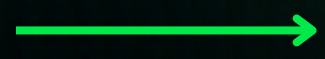
  `intext:password ext:log`

- Find vulnerable web servers. Feel free to change the POC:

  `inurl:/proc/self/cwd`

- Find excel documents that contain email addresses:

  `inurl:email.xlsx ext:xlsx`



TOP SEARCH OPERATORS FOR DORKING

Operator	Explanation	Syntax	Example
()	Group multiple terms or operators. Allows advanced expressions	(<term> or <operator>)	inurl:(html | php)
*	Wildcard. Matches any word	<text> * <text>	How to * a computer
“”	The given keyword has to match exactly. Case-insensitive	" <keywords> "	"google"
m…n / m...n	Search for a range of numbers. n should be greater than m	<number>.. <number>	1..1337
-	Documents that match the operator are excluded. NOT-Operator	- <operator>	-site:youtube.com
+	Include documents that match the operator	+ <operator>	+site:youtube.com
|	Logical OR-Operator. Only one operator needs to match in order for the overall expression to match	<operator> | <operator>	"google" | "yahoo"
~	Search for synonyms of the given word. Not supported by Google	~ <word>	~book
@	Perform a search only on the given social media platform. Rather use site	@ <socialmedia>	@instagram
after	Search for documents published / indexed after the given date	after: <yy(-mm-dd)>	after:2023-01-01

TOP SEARCH OPERATORS FOR DORKING

allintitle	Same as intitle but allows multiple keywords separated by a space	allintitle: <keywords>	allintitle:hello world
allinurl	Same as inurl but allows multiple keywords separated by a space	allinurl: <keywords>	allinurl:search com
allintext	Same as intext but allows multiple keywords separated by a space	allintext: <keywords>	allintext:math science university
AROUND	Search for documents in which the first word is up to ‘n’ words away from the second word and vice versa	<word1> AROUND(<n>) <word2>	google AROUND(10) good
author	Search for articles written by the given author if applicable	author: <name>	author:Max
before	Search for documents published / indexed before the given date	before: <yy(-mm-dd)>	before:2023-01-01
cache	Search on the cached version of the given website. Uses Google’s cache to do so	cache: <domain>	cache:google.com
contains	Search for documents that link to the given filetype. Not supported by Google	contains: <filetype>	contains:pdf
date	Search for documents published within the past ‘n’ months. Not supported by Google	date: <number>	date:3
define	Search for the definition of the given word	define: <word>	define:funny

TOP SEARCH OPERATORS FOR DORKING

ext	Search for a specific filetype	ext: <documenttype>	ext:pdf
filetype	Refer to ext	filetype: <documenttype>	filetype:pdf
inanchor	Search for the given keyword in a website's anchors	inanchor: <keyword>	inanchor:security
index of	Search for documents containing direct downloads	index of: <term>	index of:mp4 videos
info	Search for information about a website	info: <domain>	info:google.com
intext	Keyword needs to be in the text of the document	intext: <keyword>	intext:news
intitle	Keyword needs to be in the title of the document	intitle: <keyword>	intitle:money
inurl	Keyword needs to be in the URL of the document	inurl: <keyword>	inurl:sheet
link / links	Search for documents whose links contain the given keyword. Useful for finding documents that link to a specific website	link: <keyword>	link:google
location	Show documents based on the given location	location: <location>	location:UK

TOP SEARCH OPERATORS FOR DORKING

numrange	Refer to ‘m…n’	numrange: <number>-<number>	numrange:1-1337
OR	Refer to ‘|’	<operator> OR <operator>	"google" OR "yahoo"
phonebook	Search for related phone numbers associated with the given name	phonebook: <name>	phonebook:"elon musk"
relate / related	Search for documents that are related to the given website	relate: <domain>	relate:google.com
source	Search on a specific news site. Rather use site	source: <news>	source:theguardian
site	Search on the given site. Given argument might also be just a TLD such as com, net, etc	site: <domain>	site:google.com
stock	Search for information about a market stock	stock: <stock>	stock:Microsoft
weather	Search for information about the weather of the given location	weather: <location>	weather:Paris

www.blackhatethicalhacking.com