OSINT Cheat Sheet

Google Hacking

Google dorking, also known as **Google hacking**, can return information that is difficult to locate through simple search queries. Using this technique, information not intended for public access can be discovered.

The **Google Hacking Database** (GHDB) is an authoritative source for querying the ever-widening reach of the Google search engine.
Its contents are search terms, which allow to find usernames, passwords, and even files containing sensitive information. The GHDB is located here: https://www.exploit-db.com/google-hacking-database/

Google and Bing Search Operators

Operator	Description
"Search Term"	Search for the exact phrase within **" "**
-	Remove pages that mention a given term from the search results
+	Force Google to return common words that might ordinarily be discarded
OR	Search for a given search term OR another term
site:	Search within a given domain
filetype:	Search for a certain file type
intitle:	Search for sites with the given word(s) in the page title
inurl:	Search for sites with the given word(s) in the URL
intext:	Search for sites with the given word(s) in the text of the page
inanchor:	Search for sites that have the given word(s) in links pointing to them
cache:	Show most recent cache of a webpage
IP:	**Bing only:** Finds results based on a given IP address
linkfromdomain:	**Bing only:** Search for links on the given domain

Additional Google Features

Search Tools: The "Tools" button present a new row of options, which allows narrowing downs the search results. One of the most interesting options of this feature is "Custom Range", which can be used to search within a given time frame.

Google Images: The most powerful reverse image search service. https://images.google.com/

Searching for Archived Information

Google and Bing: both search engines offer a cached view of results

The Wayback Machine: http://archive.org/web/

Archive Today: http://archive.is/

Yandex

Yandex operates the largest search engine in Russia with about 65% market shares.

Yandex Search Operators

Example	Description
"I * music"	Find all results with any word where the asterisk (*) is located
Cheshire cat | hatter | Alice	Search for any word in query. This query works for Google as well
croquet +flamingo	This query would mandate that the page has the word flamingo, but not croquet
rhost:org.wikipedia.*	Reverse host search
mime:pdf	Search for specific file type
!Curiouser !and !curiouser	Search for multiple identical words
Twinkle twinkle little -star	Exclude “star” from search results
lang:en	Narrow search by language
date:200712*, date:20071215..20080101, date:>20091231	Narrow search by date or date range

Search Engines: Other Alternatives

carrot2.org: Carrot2 is a clustering search engine that groups search results into sets of topics

www.exalead.com/search: Exalead works well in finding documents that contain the search term

millionshort.com: Million Short allows removing results, which link to the one million most popular websites

globalfilesearch.com: the site claims to have indexed 243 terabytes of files stored on public FTP servers

Shodan - https://www.shodan.io

Shodan is a search engine for finding Internet-connected devices and device types. It allows searching for webcams, routers, IoT/SCADA devices, and more.

Shodan Filters

Filter	Description
city:	Search for results in a given city
country:	Search for results in a given country (2-letter code)
port:	Search for a specific port or ports
hostname:	Search for values that match the hostname
net:	Search a given IP or subnet (e.g.: 192.168.1.0/24)
product:	Search for the name of the software identified in the banner
version:	Search for the version of the product
os:	Search for a specific operating system name
title:	Search in the content scraped from the HTML tag
html:	Search in the full HTML contents of the returned page

Social Networks

Facebook

Search bar: allows searching for all profiles, which have been created using a given email address or telephone number.

Facebook ID: the Facebook UserID can be found by using https://findmyfbid.com. Alternatively, while logged into Facebook, the UserID can be found in the HTML source code after the fb://profile/ tag.

Facebook Graph Search

Result	Query
Places **Places visited** **Places recently visited** **Places checked in** **Places liked**	/search/**UserID**/places /search/**UserID**/places-visited /search/**UserID**/recent-places-visited /search/**UserID**/places-checked-in /search/**UserID**/places-liked
Pages liked	/search/**UserID**/pages-liked
Photos **Photos of** **Photos by** **Photos liked** **Photos commented**	/search/**UserID**/photos /search/**UserID**/photos-of /search/**UserID**/photos-by /search/**UserID**/photos-liked /search/**UserID**/photos-commented
Apps used	/search/**UserID**/apps
Videos **Videos of** **Videos by** **Videos liked** **Videos commented**	/search/**UserID**/videos /search/**UserID**/videos-of /search/**UserID**/videos-by /search/**UserID**/videos-liked /search/**UserID**/videos-commented
Events **Events joined in 2010**	/search/**UserID**/events /search/str/**UserID**/events-joined/2010/date/events/intersect/
Posts **Posts tagged** **Posts liked** **Posts by year**	/search/**UserID**/stories-by /search/**UserID**/stories-tagged /search/**UserID**/stories-liked /search/**UserID**/stories-by/2010/date/stories/intersect
Friends **Relatives** **Followers** **Groups** **Employers** **Co-workers**	/search/**UserID**/friends /search/**UserID**/relatives /search/**UserID**/followers /search/**UserID**/groups /search/**UserID**/employers /search/**UserID**/employees
Page likers	/likers

Additional Facebook graph queries can be found on:

- https://inteltechniques.com/osint/menu.facebook.html
- http://researchclinic.net/graph.html

Twitter Search Operators

Operator	Find Tweets…
twitter search	Containing both "twitter" and "search". This is the default operator
"happy hour"	Containing the exact phrase "happy hour"
love OR hate	Containing "love" or "hate" (or both)
beer -root	Containing "beer" but not "root"
#haiku	Containing the hashtag "haiku"
from:alexiskold	Sent from user "alexiskold"
to:techcrunch	Sent to user "techcrunch"
@mashable	Referencing user "mashable"
"happy hour" near:"san francisco"	Containing the exact phrase "happy hour" and sent from "san francisco"
near:NYC within:15mi	Sent from 15 miles of "NYC"
superhero since:2010-12-27	Containing "superhero" and sent since date "2010-12-27" (year-month-day)
ftw until:2010-12-27	Containing "ftw" and sent up to date "2010-12-27"
hilarious filter:links	Containing "hilarious" and linking to URLs
news source:"Twitter Lite"	Containing "news" and entered via Twitter Lite
geocode:47.37,8.541,10km	Sent from 10km from Zurich

Additional Twitter queries can be found on:

- https://twitter.com/search-advanced
- https://inteltechniques.com/osint/twitter.html

Social Networks User Enumeration

Through different features, it is possible to enumerate registered users:

	Twitter	Facebook	Instagram	LinkedIn	Xing
Registration	X	X	X	X	X
Password forgotten	X	X	X	X	X
Search bar		X			

The password forgotten feature of Facebook and Twitter also discloses the last two digits of the registered mobile number. This information can be used for further research.

Tools

Maltego	Maltego is an extremely powerful OSINT framework, covering infrastructural and personal reconnaissance.
FOCA	FOCA is a tool, which mainly finds metadata and hidden information in scanned documents. These documents may be found on web pages and can be downloaded and analyzed with FOCA. (https://www.elevenpaths.com)
Intel Techniques	Intel Techniques is a Swiss Army Knife for OSINT https://inteltechniques.com
Robtex	Robtex Swiss Army Knife Internet Tool. Robtex uses various sources to gather public information about IP addresses, domain names, host names, Autonomous Systems, routes, etc. The openly accessible data is indexed and stored in a database. https://www.robtex.com/

Additional Links

- **haveibeenpwned.com**: search for compromised accounts
- **dnsdumpster.com:** search for hosts related to a domain
- **crt.sh:** search in certificate transparency lists

Books

- **Google Hacking for Penetration Testers** – Johnny Long
- **Open Source Intelligence Techniques** – Michael Bazzell
- **Privacy and Security** – Michael Bazzell
- **Hiding from the Internet** – Michael Bazzell

www.compass-security.com