Cheatography

OSINT and Tools Cheat Sheet

by binca via cheatography.com/44948/cs/13288/

Google Search Engine Directives

site:	Limits results ot a target site or domain
inurl:	Searches for keywords within the URL of a page
intitle:	Searches for keywords within the title of a page.
link:	Identifies sites that link to our target, providing info that is useful for social engineering and related attacks
filetype:	Searches for files with an identifiable extension

Bing also supports site:, inurl:, intitle: and the filetype: directives.

Google Modifiers

"surroung strings in double quotes"	Literal matches for the string
- = hyphen, -site:www.domai-n.com, or -omitted	omits pages or pages with specific strings
* = asterick	Used as a keyword wildcard

Bing uses Not instead of the "-"

Google Hacking Database (GHDB)

Is a repository for search syntax, known as "Google Dorks", which can find interesting information. Works with most search engines with proper syntax adjustments.

Automate Google Searches

Google SOAP API key required for some automation tools but Google stopped issuing new keys in 12/06

Google Shunning begins with banning you from a particular search, to a 2 hour ban, to an IP ban.

SPUD by SensePost

Converts Google SOAP API requests into general searches of the Google website.

Uses "screen-scraping" to collect, parse, and return the results.

Violates Google's ToS.

Originally SensePost's Aura but that was deprecated.

Shodan

"The world's first search engine for Internet-connected devices." A plethora of devices can be found on Shodan including medical devices, traffic management systems, automotive controls, traffic light controls, HVAC/environment controls, power regulators/UPSs, security/access controls including CCTV and webcams, serial port servers and data radios.

FOCA

Search all documents in a domain

Download them

Analyze them

Produce list of metadata

Metadata collected includes users, folders, printers, software, emails, OS, password, and servers.

Supports numerous document types: doc, ppt, pps, xls, docx, pptx, ppsx, xlsx, sxw, scx, sxi, odt, ods, odg, odp, pdf, wpd, svg, svgz, indd, rdp and ica

Fingerprinting Organizations with Collected Archives is primarily a document metadata search tool, Pro is now called "Final Version."

theHarvester

Gathers information from target domains via public information sources including email addresses, IP addresses and domain names, and ports and banners.

Uses search engines, PGP key servers and Shodan

Uses screen scraping and API calls to pull results from search engines.

Maltego

Information mapping tool that finds relationships among people, sites and companies

Uses "transforms" to build a hierarchy of related information

Starting points include domain, person's name, phone number, etc.

Domain to PGP keys, Person to email, Domain to phone number

Community Edition limitations: not for commercial use, max 12 results per transform, need to register on website to use, API keys expire every couple days, runs slower, no encryption, not updated until next major version, no end user support, no updates of transforms on server sdie, only discover from Paterva servers.

Recon-ng	
Recon	>50 modules available
Mapping	0 modules overtly for mapping phase
Discovery	Cache Snoop checks the DNS cache for previously resolved names, Interesting Files looks for files of interest associated with the target
Exploi-tation	XPATH and Command Injection attacks available

Web reconnaissance framework including dozens of modules that interact with Internet services to obtain information. Reporting modules consolidate and export results, as well as discovery and exploitation modules. Some modules require API keys which may cost money. Use show info to get information about a module. 4.x update provides a significant overhaul especially of the layout and structure.

By **binca**
cheatography.com/binca/

Not published yet.
Last updated 9th November, 2017.