LLC 500 CYBERSECURITY AND ETHICAL HACKING

Linux Learning Centre Ltd

www.linuxlearningcentre.co.ke

Linux
Learning Centre

DEFINITION

Google Hacking refers to the practice of using search engines, like Google and Bing, in order to discover vulnerable web pages and critical information.

It's based on the idea that search engines index a lot of public pages and files, making their discovery a simple matter of building the correct query. Simply place the search string from a database in the Search box and you’re on your way.

It also refers to using Google to find **juicy information**, vulnerabilities, or misconfigured websites

GOOGLE DORKS

For example, it's trivial to look for a specific type of file (filetype:), on a specific domain (site:), with a specific name (inurl:), containing a certain string (intext:).

Sites: Exploit DataBase and hackersforcharity have more info on the actual queries, how they're structured, and what kind of information you can find. The SiteDigger tool gives an indication as to the type of information you can find, but is not as specific as the above mentioned sites. See also Google Hacker Tools.

https://www.exploit-db.com/google-hacking-database

GOOGLE DORKS OPERATORS

- cache: this dork will show you the cached version of any website, e.g. cache:securitytrails.com
- allintext: searches for specific text contained on any web page, e.g. allintext: hacking tools
- allintitle: exactly the same as allintext, but will show pages that contain titles with X characters, e.g. allintitle:"Security Companies"
- allinurl: it can be used to fetch results whose URL contains all the specified characters, e.g: allinurl:clientarea
- filetype: used to search for any kind of file extensions, for example, if you want to search for pdf files you can use: email security filetype: pdf
- inurl: this is exactly the same as allinurl, but it is only useful for one single keyword, e.g. inurl:admin
- intitle: used to search for various keywords inside the title, for example, intitle:security tools will search for titles beginning with "security" but "tools" can be somewhere else in the page.

GOOGLE DORKS OPERATORS

- inanchor: this is useful when you need to search for an exact anchor text used on any links, e.g. inanchor:"cyber security"
- intext: useful to locate pages that contain certain characters or strings inside their text, e.g. intext:"safe internet"
- site: will show you the full list of all indexed URLs for the specified domain and subdomain, e.g. site:securitytrails.com
- *: wildcard used to search pages that contain "anything" before your word, e.g. how to * a website, will return "how to..." design/create/hack, etc... "a website".

GOOGLE DORKS OPERATORS

- |: this is a logical operator, e.g. "security" "tips" will show all the sites which contain "security" or "tips," or both words.
- +: used to concatenate words, useful to detect pages that use more than one specific key, e.g. security + trails
- -: minus operator is used to avoiding showing results that contain certain words, e.g. security -trails will show pages that use "security" in their text, but not those that have the word "trails."