**Lab Experiment 06**

**B. Tech CSF-CSE Semester III Course: Physical and IT Security**

**By: Dr. Gopal Singh Rawat**

**Lab Objective: Use Internet to gather relevant sensitive information**

**Process: Passive Footprinting 🡪 OSINT (Open Source Intelligence)**

* **Person 🡪 gather information from Internet Social Media, Job Profile, Matrimonial Sites, Yellow Pages, Others:** 
  + [**www.Spokeo.com**](http://www.Spokeo.com)
  + [**www.411.com**](http://www.411.com)
  + [**www.PIPL.com**](http://www.PIPL.com)
* **Organization 🡪** 
  + [**www.WhoIS.net**](http://www.WhoIS.net)
  + [**www.WhoIS.com**](http://www.WhoIS.com)
  + [**www.Centralops.net**](http://www.Centralops.net)
  + [**www.SiteCheckSururi.net**](http://www.SiteCheckSururi.net)

**Search Tools:**

* **Google Search Engine**
* **GHDB**

Google has valuable resources for security researchers. For the average person, Google is just a search engine used to find text, images, videos, and news. However, in the Cybersecurity world, Google is a useful hacking tool. Although you do not go and hack sites directly using Google, but as it has tremendous web-crawling capabilities, it can index almost anything within your website, including sensitive information. This means you could be exposing too much information about your web technologies, usernames, passwords, and general vulnerabilities without even knowing it. This is Google Hack or Google Dork or Google Dorking.

**Advanced Google Operators**

|  |  |  |
| --- | --- | --- |
| **intitle:** | which finds strings in the title of a page | intitle:”Your Text” OR  intitle: “Admin Password” OR  intitle:"index of" inurl:ftp OR  intitle:index.of id\_rsa -id\_rsa.pub |
| **allintext:** | which finds all terms in the title of a page | allintext:”Contact” |
| **inurl:** | which finds strings in the URL of a page | inurl:”news.php?id=” |
| **site:** | which restricts search to a particular site or domain | site:yeahhub.com “Keyword” OR  site: upes.ac.in “Cybersecurity” |
| **filetype:** | which finds specific types of files (doc, pdf, mp3 etc) based on file extension | filetype:pdf “Cryptography” OR  filetype:xls inurl:"email.xls" |
| **link:** | which searches for all links to a site or URL | link:”example.com” |
| **cache:** | which displays Google’s cached copy of a page | cache:yeahhub.com |
| **info:** | which displays summary information about a page | info:www.example.com |

Examples

* Search Live Cameras: inurl:top.htm inurl:currenttime
* Webcams based on Transmissions: inurl:top.htm inurl:currenttime
* General Live Cameras: inurl:"lvappl.htm"
* Fetch Weather Information: intitle:"Weather Wing WS-2"

**Google Hacking Database (GHDB)**

This is a portal with search terms that have been found to reveal sensitive data exposed by vulnerable servers and web applications. The GHDB was launched in 2000 by Johnny Long to serve penetration testers.

Link 🡪 [www.exploit-db.com/google-hacking-database](http://www.exploit-db.com/google-hacking-database)

**Lab #06 File Work:**

1. Perform this Experiment to search sensitive / interesting information on the Internet using mentioned Google Operators and GHDB and mention steps/screenshots.
2. Report details about those targets as per the below table for at least 5 different targets.

|  |  |
| --- | --- |
| **Search Target** | **Information Obtained** |
| E.g. Document | Mention steps and screenshots you followed to gather that critical information |
| E.g. Domain |  |
|  |  |

Bonus: Ways to prevent Google dorks.