**Ass – 8 Google Dorking**

**🔍 What is Google Dorking?**

**Google Dorking** (also known as **Google Hacking**) is a technique that uses **advanced Google search operators** to find **sensitive information** that is **publicly available on the internet**, but not easily found with normal search queries.

It’s often used in **cybersecurity, ethical hacking, and threat intelligence** to uncover misconfigured servers, exposed login portals, sensitive files, or metadata leaks.

**✅ Simple Explanation:**

Imagine Google as a very smart detective. Normally, people just ask it simple questions. But with **Google Dorking**, you give it **very precise instructions**—like:

“Show me Excel files on this government site with passwords in them.”

This is done using **special search commands** like filetype:, inurl:, intitle:, etc.

**🛠️ Common Google Dork Operators:**

| **Operator** | **Description** |
| --- | --- |
| site: | Limits search to a specific site.  Example: site:gov.in |
| filetype: | Looks for specific file types.  Example: filetype:pdf |
| inurl: | Searches for keywords in the URL.  Example: inurl:admin |
| intitle: | Searches for keywords in the page title.  Example: intitle:index of |
| cache: | Shows Google’s cached version of a site. |
| intext: | Searches for specific words in page content. |

**🔒 Examples of Google Dorking**

1. **Find login pages**:

inurl:login site:edu.in

1. **Find exposed Excel files**:

filetype:xls intext:"password"

1. **Discover security cameras**:

inurl:"/view.shtml"

1. **Search for database dumps**:

intitle:"index of" "db.sql"

1. **Find publicly exposed WordPress admin pages**:

inurl:wp-admin site:.org

⚠️ These queries search for **public data**. Don’t try to log in or exploit — that’s illegal. Just **observe** what's exposed and report it ethically if necessary.

**🧠 Why Is Google Dorking Useful in Cybersecurity?**

* **Footprinting**: Gathering open-source intel about a target.
* **Identifying Vulnerabilities**: Finding misconfigured or forgotten endpoints.
* **Threat Intelligence**: Knowing what’s exposed can help organizations secure it.
* **Reconnaissance**: Part of the early stages of ethical hacking or penetration testing.

**🧪 How to Do Your Assignment (Safely and Legally)**

**🔹 Objective:**

Use tools like **Google Dorking** or **Shodan** to gather information about a **target** (within legal and ethical limits).

**🔹 Steps to Follow:**

**✅ Step 1: Choose a public and legal target**

Pick a **public organization website** or your own college website (e.g., site:abcuniversity.ac.in) for ethical practice.

**✅ Step 2: Use Google Dorks like:**

site:abcuniversity.ac.in filetype:pdf

site:abcuniversity.ac.in inurl:admin

site:abcuniversity.ac.in intitle:"index of"

**✅ Step 3: Document what you find**

For each dork:

* Mention the dork used
* Paste a screenshot or URL of your findings
* Describe briefly what the page shows (e.g., login portal, exposed directory)

**✅ Step 4: Mention ethical note**

State clearly:

* You did **not** access or misuse any restricted area
* This is **public info**
* The goal was **educational**

**📄 Sample Report Snippet**

🔍 Google Dork Used:

inurl:admin site:abcuniversity.ac.in

🔗 Result:

https://abcuniversity.ac.in/admin/login

📝 Description:

This shows an admin login portal of the university website.

🔐 Ethical Note:

Only public pages were visited. No login attempts or exploitation was done. This is for cybersecurity learning only.

**⚠️ Important Legal Warning**

Google Dorking is **not illegal** if used to view **already public data**, **without logging in**, and **without exploiting** any system.

❗️ Never:

* Try default passwords
* Download sensitive files
* Login without permission
* Use it on private individuals