Hello Everyone! In this video, you will learn about Google Dorks also known as Google Hacking. This is a searching technique to find out the files, information, which may not be available for the users normally.

To most users, the internet is what they experience through their email client and web browser every day, but there are a number of expansive services that operate in the background and the "web" is just one part of it. Behind that web browser, there are multiple layers that the average user may encounter indirectly or never. The web is commonly divided into the Surface Web, the Dark Web, and the Deep Web.

- **The Surface Web** is what users' access in their regular day-to-day activity. It is available to the general public using standard search engines and can be accessed using standard web browsers that do not require any special configuration, such as Mozilla Firefox, Microsoft's Internet Explorer or Edge, and Google Chrome.

- **The Deep Web** is the portion of the web that is not indexed or searchable by ordinary search engines. Users must log in or have the specific URL or IP address to find and access a particular website or service. Some pages are part of the Deep Web because they do not use common top-level domains (TLDs), such as .com, .gov, and .edu, so they are not indexed by search engines, while others explicitly block search engines from identifying them. The information stored in these pages updates frequently and is presented differently based on a user’s permissions.

- **The Dark Web** is defined as a layer of information and pages that you can only get access to through so-called "overlay networks", which run on top of the normal internet and obscure access. You need special software to access the Dark Web because a lot of it is encrypted, and most of the dark web pages are hosted anonymously.

So ,what are Google Dorks ?

- Google dorks are special search terms that are used to access specific sets of information that are not available with normal queries.

- Google Dorking can return information that is difficult to locate through simple search queries. It includes information that is not intended for public viewing but also not being adequately protected.

You can find.

- Admin login pages
- Username and passwords

- Vulnerable entities
- Sensitive documents
- Govt/military data
- Email lists
- Bank account details and lots more

Using Google Dorks if proper security measures have not been implemented on the target machines.

The main functions of Google Dorks are:

- **Intitle:** This allows to search for pages with specific text in their HTML title. So intitle: "login page" will search the web for login pages.

- **Inurl:** This allows to search for pages based on the text contained in the URL (i.e., "login.php").

- **Intext:** This operator searches the entire content of a given page for keywords supplied by the hacker.

- **Site:** This limits the scope of a query to a single website. Using the advanced "site:" search operator, it is possible to restrict search results to a specific domain

- **filetype:** Searched for certain file type. **Example:** ***filetype:pdf*** will search for all the pdf files in the websites.

- **ext:** It works similar to filetype. **Example:** ***ext:pdf*** finds pdf extension files.

- **Cache:** This will show you cached version of any website. **Example:** ***cache: aa.com***

- **Wlildcard character *:** This works like a wildcard. **Example:** ***How to * sites***, will show you all the results like *"how to…" design/create/hack, etc… "sites"*

Now the question comes in our mind is, are google dorks illegal ? Google dorks are completely legal as it's just another form of searching after all. Google was built to handle advanced searches, and banning this functionality would limit information access. But Google Dorks can quickly become illegal if they're used to surreptitiously access someone else's device, log in to someone else's account, or access or download protected files or documents. Searching for information may not be illegal but using it for unauthorized purposes almost certainly is.

In this exercise, we have created a Bash script to automate the process of searching for vulnerabilities using Google dorks.

****For further steps you can follow Lab Manual****

Thank You…