**DAY-4**

**INFORMATION GATHERING**

Information gathering is also known as **footprinting** or **reconnaissance.**

Footprinting is a collection of every possible information regarding the target and the network

**Objectives of footprinting:**

1. To know the security poster of target

2. To reduce focus area

3. Identify vulnerabilities

4. Draw the network map

**Footprinting methodologies/techniques:**

1. Footprinting using search engines

2. Footprinting using advanced google hacking techniques

3. Footprinting using social networking sites

4. Footprinting using official websites

5. Footprinting using emails

6. Footprinting using who is lookup

7. Footprinting using DNS

8. Footprinting the target network

9. Footprinting using social engineering

10. Footprinting using shodan.io/osintframework.com

**1. Footprinting using search engines:**

There are many search engines like Google, Bing, Yahoo, Duckduckgo, Yandex, CC search, Swisscows, StartPage, Search Encrypt, Gibiru, Onesearch, wiki.com, Boardreader, giveWater, Ekoru, Ecosia, Brave, Neeva, Qwant, Unsplash, Slideshare, Creative Commons Search, Listen Notes, Giphy, Dogpile, WolframAlpha, Gigablast, Keyhole, socialmention, buzzsumo, blog search engine, Scribd, flickr, pinterest, TinEye, openverse, etc.

Different search engines gathers information from different sources

Try searching your name on these different search engines

**2. Footprinting using advanced google hacking techniques**

**Google Dorks:**

A Google Dork, also known as Google Dorking or Google hacking, is a valuable resource for security researchers.

Well, you can't 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.

Refer : [Top 20 Google Hacking Techniques - Best Google Dorks and Hacks (securitytrails.com)](https://securitytrails.com/blog/google-hacking-techniques)

Some of the google dorks are:

**3. Footprinting using social networking sites**

Search for the information in social networking platforms like facebook, Instagram, twitter, etc.

You can use a web tool called **social-searcher.com**

**4. Footprinting using official websites**

**Cyotek webcopy** tool helps to download the web pages in raw formats which are publicly available.

It performs website crawling technique to find all the links in the websites.