**EXPERIMENT-02**

**FOOTPRINTING /RECONNAISANCE:**

**AIM: To study about reconnaissance and its tools**

**THEORY:**

Footprinting is the first step which lets penetration testers gather information about hardware or network. It is basically an exploration process which helps us to know our enemy. In order to complete the penetration process, one ought to gather as much information as possible.  Footprinting can be done either actively or passively. Assessing a company’s website with their permission is an illustration of passive footprinting and trying to access sensitive information through social engineering is an illustration of active information gathering.

**Active Reconnaissance**

Active footprinting means to perform footprinting by getting in direct touch with the target machine.

**Passive Reconnaissance:**

Passive foot printing means collecting information of a system located at a remote distance from the attacker.

What kind of information can be gathered from Footprinting?

1. Operating system of the target machine.
2. Firewall.
3. IP address.
4. Network map.
5. Security configurations of the target machine.
6. Email id, password.
7. Server configurations.
8. URLs.
9. VPN.

**Procedure:**

* **Footprinting through Search Engine**

Attackers use search to gather information about their target such as technology platforms, employee details, login pages, intranet portals, etc. which helps in performing social engineering and/or other types of advanced system attacks.

Even search engine cache and internet archives may provide sensitive information that has been removed from the World Wide Web (WWW).

There are many search engines where you can find anything that desires from finding the meaning of the word to finding a person. Such search engines are:

1. [www.google.com](https://www.google.com/)
2. [www.bing.com](https://www.bing.com/)
3. [www.shodan.io](https://www.shodan.io/)
4. [www.duckduckgo.com](https://www.duckduckgo.com/)

* **Footprinting through Social Networking Sites**

Attackers use social networking sites like Facebook, Twitter, and Pinterest etc. to gain important and sensitive data about their target. They often create fake profiles through these social media to lure their target and extract vulnerable information.

Employees may post personal information such as DOB, educational and employment background, spouse’s names, etc. and information about their company such as potential clients and business partners, trade secrets of business, websites, company’s upcoming news, mergers, acquisitions, etc.

Even the information about the employee’s interest is tracked and then they are trick into revealing more information.

Now if you want to search a particular person using just their name or email then there are specialized websites for it like **pipl.com and lullar.com**

* **Footprinting through Social Engineering**

Social engineering is an art of manipulating human behavior to our own advantage. This proves most helpful when the need for extraction of confidential information. To do so, we have to depend on the fact that people are unaware of their valuable information and have no idea about being exploited. The most common example for this is when people call as fake credit/debit card companies and try to extract information.

Techniques used for social engineering are:

Eavesdropping

Shoulder surfing

Dumpster diving

Impersonation on social networking sites

This is how footprinting is done through search engines, social networking sites and social engineering.

**Result:**

As white hat hackers, we should know about it but we should also be aware try to protect ourselves from black hat hackers against foot printing.