Footprinting

Footprinting is the first step of hacking. It refers to extracting information about the target. It's reconnaissance that the hacker performs to gather as much information from the computer he plans on hacking into. It contains information such as email id, passwords, type of operating system etc.

We share everything on social media and we mean everything! This provides easy information to hackers!

While this may seem like a cute way to preserve all your memories, hackers can use this information to easily know your laptop's credentials. Now... you wouldn't want a hacker to have access to your computer, would you?

In the world of Cyber Security, Footprinting is the first step which lets penetration testers gather information about hardware or network.

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.

Let's look at a few types of footprinting

1. Footprinting through Search Engine
2. Footprinting through Social Networking Sites
3. Footprinting through social engineering
4. Footprinting using advanced Google hacking techniques

Foot Printing 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.

The most common example for this is when people call as fake credit/debit card companies and try to extract information.

What is DNS Footprinting?

DNS is a naming system for computers that converts human-readable domain names into computer readable IP-addresses and vice versa.

Resource records responded by the name servers should have the following fields:

1. Domain Name - Identifying the domain

name or owner of the records

2. Record Types - Specifying the type of data in the resource record

3. Record Class Identifying a class of - network or protocol family in use

4. Time to Live (TTL) - Specifying the amount of time a record can be stored in cache before discarded.

5. Record Data - Providing the type and class dependent data to describe the resources.

DNS servers perform zone transfers to keep themselves up to date with the latest information. A zone transfer of a target domain gives a list of all public hosts, their respective IP addresses, and the record type.