FOOTPRINTING

INTRODUCTION

Footprinting is a part of the reconnaissance process which is used for gathering possible information about a target computer system or network. Footprinting could be both passive and active. Reviewing a company's website is an example of passive footprinting, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.

During this phase, an you can collect the following information

- DOMAINE NAME
- EMAIL ADDRESS
- PHONE NUMBER
- EMPLOYEES INFOS
- IP ADDRESS
- AND MORE

General footprinting is really simple and even an everyday user could do it using websites like whois.com, ip2location.com, archive.org etc

ACTIVE FINGERPRINTING

Active fingerprinting is having contact with the target accomplished by sending specially crafted packets to a target machine and then noting down its response and analyzing the gathered information to determine the target OS.

PASSIVE FINGERPRINTING

Passive fingerprinting is based on sniffer traces from the remote system. Based on the sniffer traces (such as Wireshark) of the packets, you can determine the operating system of the remote host. Before attacking a system, you need to know what operating system is hosting a website. Once a target OS is known, then it becomes easy to determine which vulnerabilities might be present to exploit the target system. Fingerprinting is done by analyzing various factors of a packet

FOOTPRINTING HELPS TO :

- **Know Security Posture** The data gathered will help you to get an overview of the security posture of the company such as details about the presence of a firewall, security configurations of applications etc.

- **Reduce Attack Area** Can identify a specific range of systems and concentrate on particular targets only. This will greatly reduce the number of systems you are focussing on.

- **Identify vulnerabilities** you can build an information database containing the vulnerabilities, threats, loopholes available in the system of the target organization.

- **Draw Network map** helps to draw a network map of the networks in the target organization covering topology, trusted routers, presence of server and other information.

GOOGLE HACKING

Google hacking refers to collecting information using google dorks (keywords) by constructing search queries which result in finding sensitive information.details collected include compromised passwords, default credentials, competitor information, information related to a particular topic etc.

WHOIS FOOTPRINTING

Whois databases and the servers are operated by RIR - Regional Internet Registries. These databases contain the personal information of Domain Owners. Whois utility interrogates the Internet domain name administration system and returns the domain ownership, address, location, phone numbers, and other details about a domain name.

FOOTPRINTING THOUGH SOCIAL MEDIA

Social media like twitter, facebook, instagram ... are searched to collect information like personal details, user credentials, other sensitive information using various social engineering techniques. Some of the techniques include

- **Eavesdropping**: It is the process of intercepting unauthorized communication to gather information

- **Shoulder surfing**: Secretly observing the target to gather sensitive information like passwords, personal identification information, account information etc

- **Dumpster Diving**: This is a process of collecting sensitive information by looking into the trash bin. Many of the documents are not shredded before disposing them into the trash bin . Retrieving these documents from trash bin may reveal sensitive information regarding contact information, financial information, tender information etc.

Footprinting countermeasures

- Creating awareness among the employees and users about the dangers of social engineering
- Limiting the sensitive information
- encrypting sensitive information
- using privacy services on whois lookup database
- Disable directory listings in the web servers
- Enforcing security policies