



SNS COLLEGE OF ENGINEERING

Coimbatore-35
An Autonomous Institution



Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF CSE (IoT & Cyber Security including Blockchain Technology)

19SB502 – CYBER FORENSIC AND INVESTIGATIONS

III YEAR/ V SEMESTER

UNIT 4 – ETHICAL HACKING

TOPIC 4 –2 Foot printing

10/21/2024



INTRODUCTION OF FOOTPRINTING

Footprinting is an [ethical hacking](#) technique used to gather as much data as possible about a specific targeted computer system, an infrastructure and networks to identify opportunities to penetrate them. It is one of the best methods of finding vulnerabilities.

The process of cybersecurity footprinting involves profiling organizations and collecting data about the network, host, employees and third-party partners. This information includes the [OS](#) used by the organization, [firewalls](#), network maps, [IP addresses](#), [domain name system](#) information, security configurations of the target machine, [URLs](#), [virtual private networks](#), staff IDs, email addresses and phone numbers.





Types of Footprints

a) **Active Footprinting:** It means performing footprinting by getting indirect touch with target machine.

b) **Passive Footprinting:** It means collecting information about a system located at remote distance from the attacker



What is active & passive footprinting?

- Active footprinting describes the process of using tools and techniques, like using the [traceroute](#) commands or a ping sweep -- [Internet Control Message Protocol sweep](#) -- to collect data about a specific target. This often triggers the target's intrusion detection system ([IDS](#)). It takes a certain level of stealth and creativity to evade detection successfully.
- Passive footprinting involves collecting data about a specific target using innocuous methods, like performing a Google search, looking through Archive.org, using NeoTrace, browsing through employees' social media profiles, looking at job sites and using Whois, a website.





ACTIVE VS PASSIVE DIGITAL FOOTPRINT



ACTIVE

- Social Media Posts
- Online comments
- Shopping preferences
- Photos and Videos
- Location Data

PASSIVE

- Social Security Number
- Tax Records
- IP address
- Browsing history
- Device information



What Information Is Collected in Footprinting?

The goal of footprinting is to gather as much information about the target as possible in order to increase the likelihood of success when actually planning and executing an attack. This includes identifying any security weaknesses and gathering contact information for system administrators and other users who may access sensitive data. During footprinting, various types of information may be collected

- OS used by the organization,
- firewalls, network maps,
- IP addresses,
- domain name system information,
- security configurations of the target machine,
- URLs, virtual private networks, staff IDs,
- email addresses and phone numbers.



Digital footprint examples

- **Social media sites**
 - Social media credentials connecting other websites
 - Posting pictures and sharing data on social accounts
 - Communicating with friends and other contacts
- **Online Banking**
 - Use of a mobile application for online banking
 - Getting subscriptions to blogs and financial publications
 - Requesting a credit card account
- **Health**
 - Use of fitness trackers and wearable tech
 - Using an email address for a gym registration
 - Getting a subscription to health and fitness blogs



What are the steps of footprinting?

- Information gathering.
- Determining the range of the network.
- Identifying active machines.
- Identifying open ports and access points.
- OS fingerprinting.
- Fingerprinting services.
- Mapping the network.





Advantages of Footprinting

- 1) It allows hackers to gather the basic security configurations of target machine.
- 2) It is best method of vulnerabilities.
- 3) By using this hacker identify as to which attacker is handier to hack the target system.





THANK YOU