


What is Footprinting?

Footprinting is the first step of any attack on information systems in which an attacker **collects information about a target network** to identify various ways to intrude into the system

Types of Footprinting	Information Obtained in Footprinting	Objectives of Footprinting
<ul style="list-style-type: none">● Passive Footprinting<ul style="list-style-type: none">⊕ Gathering information about the target without direct interaction● Active Footprinting<ul style="list-style-type: none">⊕ Gathering information about the target with direct interaction	<ul style="list-style-type: none">● Organization information<ul style="list-style-type: none">⊕ Employee details, telephone numbers, location, background of the organization, web technologies, etc.● Network information<ul style="list-style-type: none">⊕ Domain and sub-domains, network blocks, IP addresses of the reachable systems, Whois record, DNS, etc.● System information<ul style="list-style-type: none">⊕ OS and location of web servers, users and passwords, etc.	<ul style="list-style-type: none">● Knowledge of security posture● Reduction of focus area● Identifying vulnerabilities● Drawing of network map 

What is Footprinting?

An essential aspect of footprinting is identifying the level of risk associated with the organization's publicly accessible information. Footprinting, the first step in ethical hacking, refers to the process of collecting information about a target network and its environment. Using footprinting, you can find a number of opportunities to penetrate and assess the target organization's network.

After you complete the footprinting process in a methodological manner, you will obtain the blueprint of the security profile of the target organization. Here, the term "blueprint" refers to the unique system profile of the target organization acquired by footprinting.

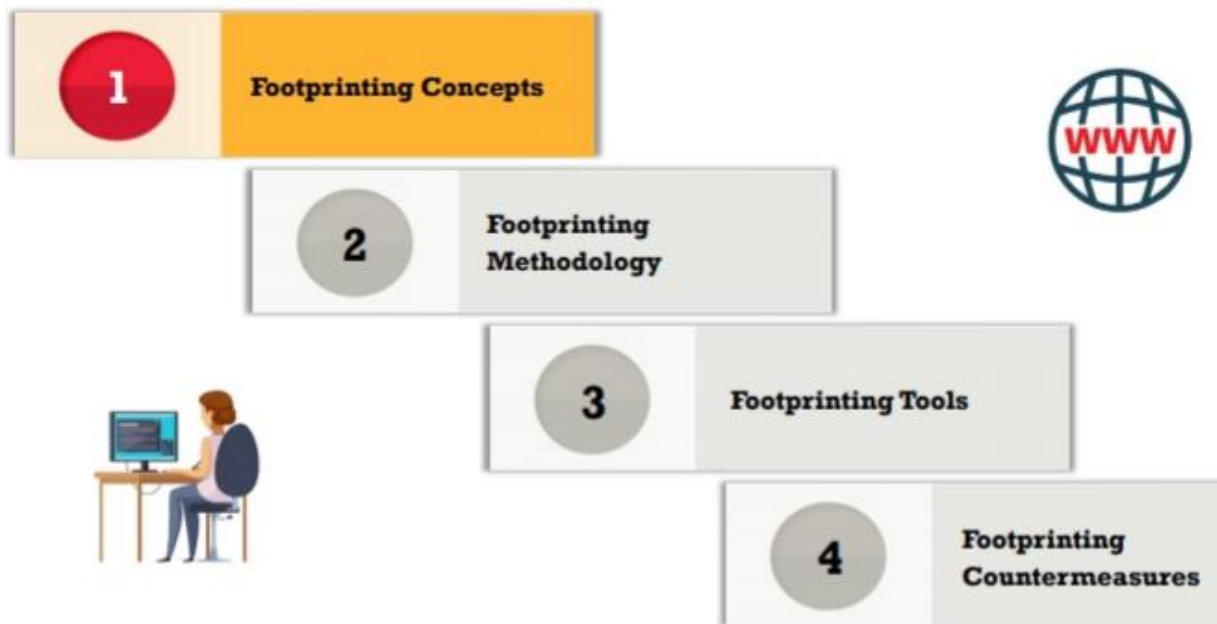
There is no single methodology for footprinting, as information can be traced in a number of ways. However, the activity is important, as you need to gather all the crucial information about the target organization before beginning the hacking phase. For this reason, footprinting needs to be carried out in an organized manner. The information gathered in this step helps in uncovering vulnerabilities existing in the target network and in identifying different ways of exploiting these vulnerabilities.

Footprinting Concepts

Ethical hacking is legal in nature and conducted to evaluate the security of a target organization's IT infrastructure with their consent. Footprinting, where an attacker tries to gather information about a target, is the first step in ethical hacking. This step acts as a preparatory phase for the attacker, who needs to gather as much information as possible to easily find ways to intrude into the target network.

This section aims to familiarize you with footprinting, why it is necessary, and its objectives.

Module Flow



Types of Footprinting

Footprinting can be categorized into passive footprinting and active footprinting.

- **Passive Footprinting**

Passive footprinting involves gathering information about the target without direct interaction. It is mainly useful when the information gathering activities are not to be detected by the target. Performing passive footprinting is technically difficult, as active traffic is not sent to the target organization from a host or anonymous hosts or services

over the Internet. We can only collect archived and stored information about the target using search engines, social networking sites, and so on.

Passive footprinting techniques include:

- Finding information through search engines
- Finding the Top-level Domains (TLDs) and sub-domains of a target through web services
- Collecting location information on the target through web services
- Performing people search using social networking sites and people search services
- Gathering financial information about the target through financial services
- Gathering infrastructure details of the target organization through job sites
- Collecting information through deep and dark web footprinting
- Determining the operating systems in use by the target organization
- Performing competitive intelligence
- Monitoring the target using alert services
- Gathering information using groups, forums, blogs, and NNTP Usenet newsgroups
- Collecting information through social engineering on social networking sites
- Extracting information about the target using Internet archives
- Gathering information using business profile sites
- Monitoring website traffic of the target
- Tracking the online reputation of the target

Active Footprinting

Active footprinting involves gathering information about the target with direct interaction. In active footprinting, the target may recognize the ongoing information gathering process, as we overtly interact with the target network. Active footprinting requires more preparation than passive footprinting, as it may leave traces that may alert the target organization.

Active footprinting techniques include:

- Querying published name servers of the target
- Searching for digital files
- Extracting website links and gathering wordlists from the target website
- Extracting metadata of published documents and files
- Gathering website information using web spidering and mirroring tools
- Gathering information through email tracking

- Harvesting email lists
- Performing Whois lookup
- Extracting DNS information
- Performing traceroute analysis
- Performing social engineering

Information Obtained in Footprinting

The major objectives of footprinting include collecting the network information, system information, and organizational information of the target. By conducting footprinting across different network levels, you can gain information such as network blocks, specific IP addresses, employee details, and so on. Such information can help attackers in gaining access to sensitive data or performing various attacks on the target network.

- **Organization Information:** Such information about an organization is available from its website. In addition, you can query the target's domain name against the Whois database and obtain valuable information.

The information collected includes:

- Employee details (employee names, contact addresses, designations, and work experience)
- Addresses and mobile/telephone numbers
- Branch and location details
- Partners of the organization
- Web links to other company-related sites
- Background of the organization
- Web technologies
- News articles, press releases, and related documents
- Legal documents related to the organization
- Patents and trademarks related to the organization

Attackers can access organizational information and use such information to identify key personnel and launch social engineering attacks to extract sensitive data about the entity.

Network Information: You can gather network information by performing Whois database analysis, trace routing, and so on.

The information collected includes:

- Domain and sub-domains
- Network blocks
- Network topology, trusted routers, and firewalls
- IP addresses of the reachable systems
- Whois records
- DNS records and related information

System Information: You can gather system information by performing network footprinting, DNS footprinting, website footprinting, email footprinting, and so on.

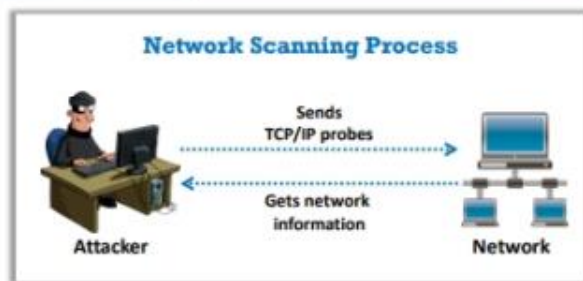
The information collected includes:

- Web server OS
- Location of web servers
- Publicly available email addresses
- Usernames, passwords, and so on.

Overview of Network Scanning



- Network scanning refers to a set of procedures used for **identifying hosts, ports, and services** in a network
- Network scanning is one of the **components of intelligence gathering** which can be used by an attacker to create a profile of the target organization



Objectives of Network Scanning

- To discover live hosts, IP address, and open ports of live hosts
- To discover operating systems and system architecture
- To discover services running on hosts
- To discover vulnerabilities in live hosts



Overview of Network Scanning

Scanning is the process of gathering additional detailed information about the target using highly complex and aggressive reconnaissance techniques. Network scanning refers to a set of procedures used for identifying hosts, ports, and services in a network. Network scanning is also used for discovering active machines in a network and identifying the OS running on the target machine. It is one of the most important phases of intelligence gathering for an attacker, which enables him/her to create a profile of the target organization. In the process of scanning, the attacker tries to gather information, including the specific IP addresses that can be accessed over the network, the target's OS and system architecture, and the ports along with their respective services running on each computer.

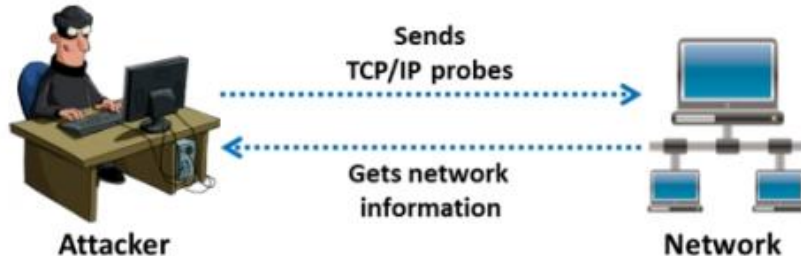


Figure 3.1: Network scanning process

The purpose of scanning is to discover exploitable communications channels, probe as many listeners as possible, and track the ones that are responsive or useful to an attacker's particular needs. In the scanning phase of an attack, the attacker tries to find various ways to intrude into a target system. The attacker also tries to discover more information about the target system to determine the presence of any configuration lapses. The attacker then uses the information obtained to develop an attack strategy.

Port and Service Discovery

The next step in the network scanning process involves checking the open ports and services in live systems. After performing a ping scan, once attackers detect the live systems in the target network, they try to find open ports and services in the discovered live systems. This discovery of open ports and services can be performed via various port scanning techniques. Administrators often use port scanning techniques to verify the security policies of their networks, whereas attackers use them to identify open ports and running services on a host with the intent of compromising the network. Moreover, sometimes, users unknowingly keep unnecessary open ports on their systems. An attacker takes advantage of such open ports to launch attacks.

This section describes the common ports and corresponding services along with various port scanning techniques and tools used by the attacker to perform port scanning.

List of Common Ports and Services

The important reserved ports are listed below:

Name	Port/Protocol	Service Description
echo	7/tcp	
echo	7/udp	
discard	9/tcp	sink null
discard	9/udp	sink null
systat	11/tcp	Users
daytime	13/tcp	

Port Scanning Techniques

Port scanning techniques are further categorized as described below. This categorization is based on the type of protocol used for communication in the network.

TCP Scanning:

- Open TCP Scanning Methods
 - TCP Connect/Full Open Scan
- Stealth TCP Scanning Methods
 - Half-open Scan
 - Inverse TCP Flag Scan
 - Xmas Scan
 - FIN Scan
 - NULL Scan
 - Maimon Scan
 - ACK Flag Probe Scan
 - TTL-Based Scan
 - Window Scan
- Third Party and Spoofed TCP Scanning Methods
 - IDLE/IP ID Header Scan

UDP Scanning:

- UDP Scanning

SCTP Scanning:

- SCTP INIT Scanning
- SCTP COOKIE/ECHO Scanning

SSDP Scanning:

- SSDP and List Scanning

IPv6 Scanning:

- IPv6 Scanning

Gaining Access

The previous phases of hacking, including footprinting and reconnaissance, scanning, enumeration, and vulnerability assessment, help attackers to identify security loopholes and vulnerabilities that exist in the target organizational IT assets. Attackers use this information, along with techniques such as cracking passwords and exploiting vulnerabilities such as buffer overflows, to gain access to the target organizational system.

Maintaining Access

After successfully gaining access and escalating privileges to the target system, attackers ensure that high levels of access are maintained to perform malicious activities such as executing malicious applications and stealing, hiding, or tampering with sensitive system files.

Clearing Logs

To maintain future system access, attackers attempt to avoid recognition by legitimate system users. To remain undetected, attackers wipe out the entries corresponding to their activities in the system logs, thus avoiding detection by users.