Footprinting and Reconnaissance

Made with Gamma

Footprinting

Footprinting and reconnaissance are the initial steps taken to gather information about a target system or network. During this phase, an attacker tries to collect as much information as possible about the target, such as IP addresses, network topology, operating systems, services running on open ports, and other system details. This information is used to identify vulnerabilities and weaknesses in the system that can be exploited later.

Active Footprinting	Passive Footprinting
Active information gathering involves direct interaction with the target system or network. This means sending requests or queries to the target with the intention of receiving responses that reveal information about the system.	Passive information gathering involves collecting data about the target system or network without direct interaction. It does not involve sending requests or queries to the target.

Made with Gamma

Information obtain in Footprinting

1 **Organization information**

Employee details

Telephone numbers

Branch and location details

Background of the organization

Web technologies

News articles, press releases, and related documents

2 **Network information**

Domain and subdomains

Network blocks

Network topology, trusted routers, and firewalls

IP addresses of the reachable systems

Whois records

DNS records

3 **System information**

Web server OS

Location of web servers

Publicly available email addresses

Usernames and passwords

Made with Gamma

Footprinting Through Search Engines

Footprinting through search engines, also known as "search engine footprinting," is a passive information-gathering technique used to collect publicly available data and information about a target organization, its employees, and its online presence. This process involves leveraging popular search engines like Google, Bing, and specialized search engines to uncover details about the target. Here are the steps

1. **Google Dorking:**
   - Google Dorking involves using advanced search operators to refine and narrow down search results. For example, site:, filetype:, intitle:, inurl:, etc., can be combined to focus on specific domains, file types, titles, or URLs.
2. **Website Enumeration:**
   - Searching for information related to the target's website can reveal valuable details. Using search engines to find subdomains, IP addresses, and associated websites can provide a broader understanding of the target's online presence.
3. **Filetype Searches:**
   - Searching for specific file types related to the target (e.g., PDFs, DOCs, XLS) can yield documents that might contain sensitive information. Using the "filetype:" operator in search engines can help narrow down the search.
4. **Social Media Profiling:**
   - Leveraging search engines to find and profile social media accounts associated with the target or its employees can provide insights into personal and professional relationships, interests, and potential security risks.
5. **Email Address Search:**
   - Searching for email addresses associated with the target domain can reveal contact information, which might be useful for social engineering or other attack vectors.
6. **Job Postings and Employee Information:**
   - Job postings on various platforms may provide details about the technology stack used by the organization. Additionally, employee profiles on professional networking sites may offer insights into roles, responsibilities, and technologies in use.
7. **Website Mirroring and Archiving:**
   - Using tools to mirror or archive websites can help preserve information even if it is later removed or changed. This can be useful for historical analysis.
8. **Reviewing Code Repositories:**
   - Searching for code repositories on platforms like GitHub or GitLab may reveal source code, configurations, or other sensitive information unintentionally exposed by the organization.
9. **News and Reviews:**
   - Searching for news articles, reviews, or mentions related to the target can provide information about security incidents, partnerships, or other relevant events.

Made with Gamma

Network based information gadhering

1. **Whois Lookup:**
   - Retrieves registration details of a domain or IP address, helping assess risks and vulnerabilities.
2. **IP Lookup:**
   - Provides geolocation, ISP, and associated domains for an IP address, offering insights into network connections.
3. **Reverse IP Lookup:**
   - Identifies domains hosted on a specific IP, aiding in understanding the network's infrastructure and finding potential vulnerabilities.
4. **Domain Lookup:**
   - Gathers registrar, registration, and expiration details of a domain, helping assess ownership and history.
5. **DNS Lookup:**
   - Retrieves DNS records associated with a domain, including IP addresses and configuration details, aiding in identifying potential weaknesses or misconfigurations.

Browser Extensions:

1. Shodan
2. WhatRuns
3. Wappalyzer

Websites for Subdomain Discovery:

1. DNSDumpster
2. Pentest-Tools
3. Spyse
4. Subdomain Finder
5. NMmapper

Server Information:

1. YouGetSignal - Reverse IP Domain Checkup
2. DomainTools - Reverse IP
3. Whois.net

Informational Websites:

1. ICANN Whois
2. MXToolbox

Check Website History:

1. Internet Archive

Made with Gamma

Target Base Information Gathering

Organization Profiling:

1. **Company Website Analysis:**
   - Gather information about the organization's products, services, mission, history, and key personnel from its official website.
2. **News and Press Releases:**
   - Review news articles and press releases to understand recent activities, achievements, and challenges.
3. **Financial Reports:**
   - Analyze financial reports (if available) for insights into the organization's financial health and performance.
4. **Social Media Accounts:**
   - Explore the organization's social media profiles for updates and announcements.

Contact Information:

1. **Email Address Enumeration:**
   - Collect known email addresses associated with the organization.
2. **Phone Number Identification:**
   - Discover phone numbers from public records or social media profiles.
3. **Publicly Available Documents:**
   - Search for documents containing contact information.

Associations and Relationships:

1. **Friends and Colleagues:**
   - Identify personal and professional relationships of key individuals.
2. **Affiliations:**
   - Discover an individual's affiliations with other organizations or groups.

Public Records and Online Archives:

1. **Public Records:**
   - Access property records, legal filings, and government documents.
2. **Internet Archive Searches:**
   - Search the Internet Archive for historical information about the organization.

Made with Gamma