

Module 2: Footprinting and Reconnaissance

 by Durgesh Thakare

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

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 Footprinting

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.

Information obtain in Footprinting

Information obtained through passive footprinting can be used to identify potential vulnerabilities in the target's system. This can include outdated software versions, weak passwords, or misconfigured settings. By gathering this information, an attacker can develop a more targeted and effective attack strategy. It is important for organizations to be aware of the potential risks associated with passive footprinting and take proactive measures to protect their sensitive information.

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 sub-domains
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

Network based information gadhering

Network-Specific Information Gathering:

Information gathering in a network-based context, often used in ethical hacking and penetration testing, involves collecting detailed data about a target network to understand its structure, devices, vulnerabilities, and potential attack vectors. Here's a deeper look into network-based information gathering:

Who is lookup A "whois" lookup is a common tool used in network-based information gathering. It allows users to retrieve registration information about a domain or IP address, including details such as the owner, contact information, and registration date. This information can be valuable in assessing the potential risks and vulnerabilities associated with a target network.

Ip-lookup Another useful tool for network-based information gathering is an "IP-lookup." This tool allows users to gather detailed information about an IP address, such as the geolocation, internet service provider (ISP), and potentially associated domains. Conducting an IP-lookup can provide valuable insights into the network's physical location and its potential connections to other systems or entities.

Reverse ip lookup A reverse IP lookup is a technique used to identify the domains that are hosted on a particular IP address. This can be helpful in discovering other websites or systems that are associated with the target network. By conducting a reverse IP lookup, an attacker can gain a better understanding of the network's infrastructure and potentially identify additional vulnerabilities or attack vectors.

Domain lookup A domain lookup is a technique used to gather information about a specific domain name. This can include details such as the registrar, registration date, and expiration date of the domain. By conducting a domain lookup, an attacker can gain insights into the ownership and history of the target domain, helping them assess potential risks and vulnerabilities in the network.

Dns lookup A DNS lookup is a technique used to gather information about the DNS records associated with a domain. This can include details such as the IP addresses linked to the domain, mail server information, and other DNS records like TXT or MX records. Conducting a DNS lookup can provide valuable information about the target domain's infrastructure and configuration, helping an attacker in identifying potential weak points or misconfigurations that could be exploited.

Browser Extension

- <https://chrome.google.com/webstore/detail/shodan/jjalcfnidlmpjhdfepjhjbhnhkbg leap>
- <https://chrome.google.com/webstore/detail/whatruns/cmkd bmfndkfgebldh nkb fhlneefdaaip>
- <https://chrome.google.com/webstore/detail/wappalyzer-technology-pro/gppongmhjkpfnbhagpmjfkannfbllamg>

Websites

Sub Domain Finder

- <https://dnsdumpster.com/>
- <https://pentest-tools.com/information-gathering/find-subdomains-of-domain#>
- <https://spyse.com/>
- <https://subdomainfinder.c99.nl/>
- <https://www.nmmapper.com/>

Server Information

- <https://www.yougetsignal.com> --> reverse IP DOMAIN CHEKUP
- <http://reverseip.domaintools.com/https://whois.net/>

Informational Websites

- <https://whois.icann.org/en>
- <https://mxtoolbox.com/>

Check Website History

- <https://archive.org/>

Target-Based Information Gathering

Target-based or person-based information gathering is an essential aspect of ethical hacking and penetration testing that focuses on collecting information about specific individuals, organizations, or entities. This type of information gathering helps ethical hackers and security professionals understand their targets, identify potential vulnerabilities, and plan security assessments or penetration tests effectively. Here's a deeper look at target-based and person-based information gathering:

Organization Profiling:

- **Company Website Analysis:** Analyzing the target organization's website to gather information about its products, services, mission, history, and key personnel.
- **News and Press Releases:** Reviewing news articles and press releases related to the organization to understand its recent activities, achievements, and challenges.
- **Financial Reports:** Analyzing financial reports, if available, to gain insights into the organization's financial health and performance.
- **Social Media Accounts:** Exploring the organization's social media profiles for updates and announcements.

Contact Information:

- **Email Address Enumeration:** Collecting known email addresses associated with the individual.
- **Phone Number Identification:** Discovering phone numbers, if available, from public records or social media profiles.
- **Publicly Available Documents:** Searching for publicly available documents containing contact information.

Associations and Relationships:

- **Friends and Colleagues:** Identifying an individual's personal and professional relationships.
- **Affiliations:** Finding out an individual's affiliations with organizations or group

Public Records and Online Archives:

- **Public Records:** Accessing public records such as property records, legal filings, and government documents.
- **Internet Archive Searches:** Searching the Internet Archive (Wayback Machine) for historical data related to an individual or their online presence.

OSINT Framework

OSINT Framework, also known as "OSINT Framework" (OSINT stands for Open-Source Intelligence), is a comprehensive online resource that provides a curated list of open-source intelligence tools, resources, and references. It is designed to assist individuals and professionals in conducting open-source intelligence activities, which involve gathering information from publicly available sources to gain insights and intelligence.

The OSINT Framework offers a well-organized and categorized collection of tools and websites that can be used for various aspects of open-source intelligence. This includes tools for data collection, information analysis, digital forensics, network reconnaissance, social media investigation, and more. Users can explore and access a wide range of resources and tools for conducting investigations, research, and intelligence gathering.

1. **Data Collection Tools:** Tools that help collect data from publicly available sources, such as search engines, social media, news, and websites.
2. **Information Analysis:** Tools for processing and analyzing the data collected, including data analysis software and tools for linguistic analysis.
3. **Digital Forensics:** Resources for digital forensics investigations, including forensic analysis tools and reference materials.
4. **Network Reconnaissance:** Tools and resources for network scanning and reconnaissance.
5. **Social Media Investigation:** Tools and techniques for investigating social media profiles and activities.
6. **Dark Web Research:** Resources for researching and monitoring activities on the dark web and hidden online communities.
7. **Geolocation and Mapping:** Tools for geolocation, mapping, and tracking activities.
8. **Phone Number Investigation:** Resources for investigating phone numbers, including reverse phone lookup services.
9. **Email Investigation:** Tools for email analysis and email tracking.
10. **Username Investigation:** Resources for investigating usernames and online identities.
11. **Miscellaneous:** A category for other relevant resources and tools that may not fit into the previous categories.

 osintframework.com



OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally (D) - Google Dork, for more information: Google Hacking (R) - Requires registration (M) - Indicates a URL that contains the search term and the URL itself must be...