

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

Types of Footprinting

Passive Footprinting

Gathering information about a target **without direct interaction**

Active Footprinting

Gathering information about the target **with direct interaction**

Information Obtained in Footprinting

Organisation Information

Employee details, telephone numbers, location, background of the organization, web technologies, etc.

Network Information

Domain and sub-domains, network blocks, IP addresses of the reachable systems, Whois record, DNS, etc.

System Information

OSes and location of web servers, users and passwords, etc.

Methodology

Footprinting techniques:

- Footprinting through search engines
- Footprinting through web services
- Footprinting through social networking sites
- Website footprinting
- Email footprinting
- Competitive intelligence
- Whois footprinting
- DNS footprinting
- Network footprinting
- Footprinting through social engineering

- Google hacking refers to the use of advanced Google search operators for **creating complex search queries** in order to extract sensitive or hidden information that helps attackers to **find vulnerable targets**

Google supports several advanced operators that help in modifying the search

[cache:] Displays the web pages stored in the Google cache

[link:] Lists web pages that have links to the specified web page

[related:] Lists web pages that are similar to a specified web page

[info:] Presents some information that Google has about a particular web page

[site:] Restricts the results to those websites in the given domain

[allintitle:] Restricts the results to those websites with all of the search keywords in the title

[intitle:] Restricts the results to documents containing the search keyword in the title

[allinurl:] Restricts the results to those with all of the search keywords in the URL


[inurl:] Restricts the results to documents containing the search keyword in the URL


[location:] Finds information for a specific location


- Social engineering is an art of exploiting human behaviour to **extract confidential information**
- Social engineers depend on the fact that **people are unaware** of their valuable information and are careless about protecting it

Footprinting
Countermeasures


CEH

**Restrict the employees** to access social networking sites from organization's network

**Configure web servers** to avoid information leakage

**Educate employees** to **use pseudonyms** on blogs, groups, and forums

**Do not reveal critical information** in **press releases, annual reports, product catalogues, etc.**

**Limit the amount of information** that you are publishing on the website/ Internet

**Use footprinting techniques** to discover and remove any sensitive information publicly available


**Prevent search engines** from caching a web page and **use anonymous registration services**


Copyright © by **CEH**. All Rights Reserved. Reproduction is Strictly Prohibited.


Footprinting
Countermeasures


CEH


Footprinting Countermeasures (Cont'd)


**Develop and enforce security policies** to regulate the information that employees can reveal to third parties


**Set apart internal and external DNS** or use split DNS, and **restrict zone transfer** to authorized servers

**Disable directory listings** in the web servers

**Conduct periodically security awareness training** to educate employees about various **social engineering tricks and risks**

**Opt for privacy services** on **Whois Lookup database**

**Avoid domain-level cross-linking** for the critical assets

**Encrypt** and **password protect** sensitive information

Copyright © by **CEH**. All Rights Reserved. Reproduction is Strictly Prohibited.