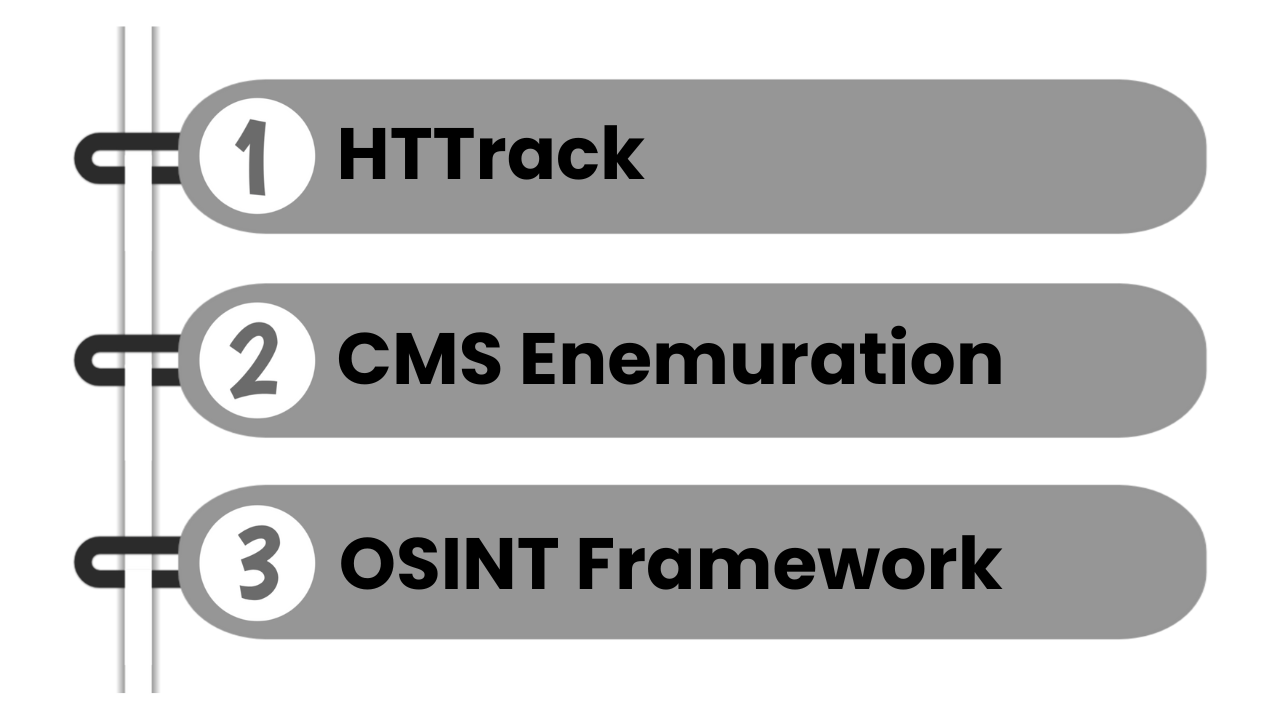


# Lesson 04: Tools for Footprinting (HTTrack, CMS Enemuration, OSINT Framework)



## Lesson Objectives

By the end of this lesson, you will be able to:

* Understand how to copy websites for offline analysis.
* Identify which CMS (Content Management System) a site uses.
* Use OSINT tools to gather public data about a person, domain, or organization.
* Apply these tools in ethical and legal ways during reconnaissance.

## 1. What Are These Tools Used For?

## 

## 

## 

## 

## 

## 1.1 HTTrack – Website Copier



### What It Does:

HTTrack downloads and saves a complete copy of a website to your computer.

### How to Use:

Command line:

* httrack http://example.com

Or use the graphical version (available for Windows and Linux).

### What You Get:

* Full offline version of the website
* Folders with HTML, images, styles, and scripts

### Good For:

* Studying how a site is structured
* Collecting content for offline analysis
* Exploring websites without interacting with the live server

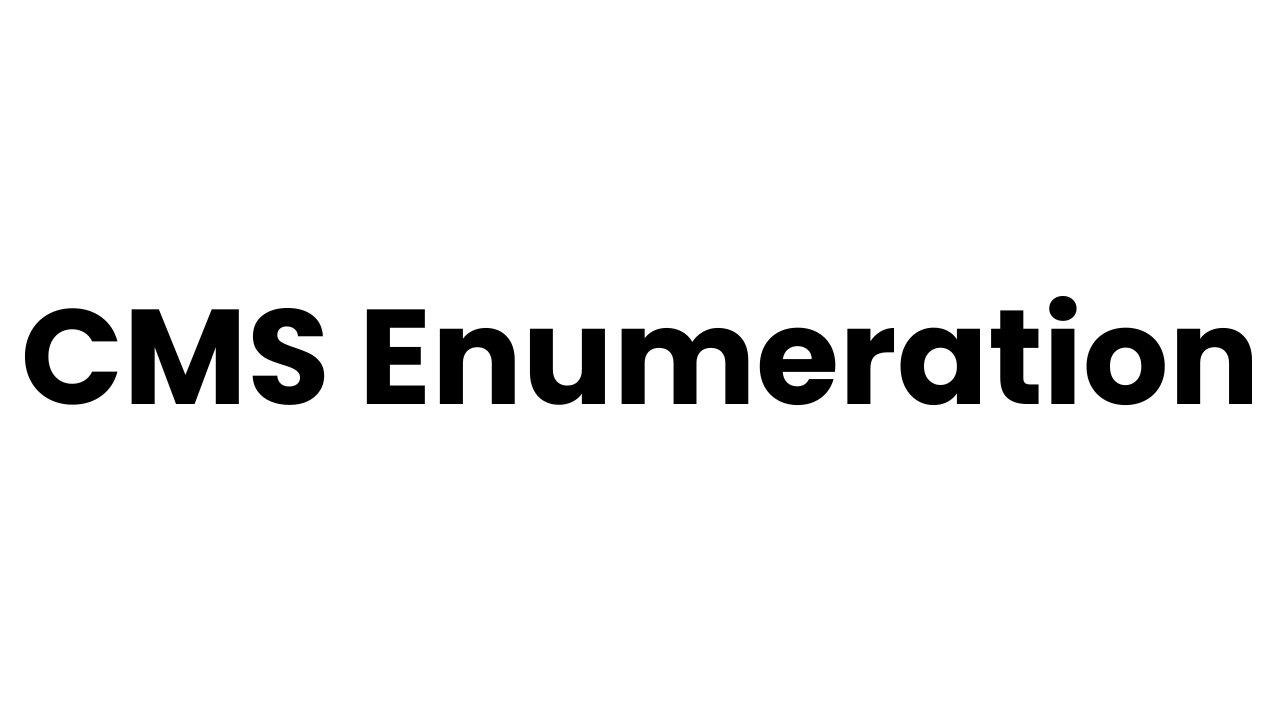
### Limitations:

* Only copies public content (not admin or backend)
* Some sites block bots or downloading

## 

## 

## 1.2 CMS Enumeration



### What It Does:

Detects which Content Management System (CMS) a website uses, such as WordPress, Joomla, or Drupal.

### Tools You Can Use:

* **WhatWeb** – general CMS detection  
    
   whatweb example.com
* **WPScan** – focused on WordPress  
    
   wpscan --url https://example.com

### What You Learn:

* CMS name and version
* Plugins or themes in use
* Known vulnerabilities (if outdated)

### Good For:

* Identifying security issues in CMS-based websites
* Preparing for penetration testing

### Limitations:

* May not detect all CMSs or plugins
* Results can vary based on the site’s security settings

## 1.3 OSINT Framework



### What It Does:

Provides a collection of free OSINT (Open-Source Intelligence) tools to gather public information.

### Website:

[https://osintframework.com](https://osintframework.com/)

### How to Use:

* Open the website
* Browse categories like:  
  + People search
  + Domain research
  + Social media
  + Breach data
  + Email investigation

### What You Can Find:

* Public data about websites, people, emails, and companies
* Links to tools for checking usernames, leaks, and more

### Good For:

* Safe, passive information gathering
* Getting a full view of a target using only public data

### Limitations:

* Results depend on how much public info exists
* Some tools may require registration or have limits

## 2. Hands-On Practice

Try these activities in a lab or test environment:

1. Use HTTrack to download and view a simple website offline.
2. Run WhatWeb or WPScan on a demo or test WordPress site.
3. Use the OSINT Framework to find data on a domain or username.

## 

## 3. Be Ethical

* Do not mirror websites without permission, especially private or commercial ones.
* Only perform CMS scanning on your own site or with written permission.
* Use OSINT tools for public data only — avoid anything illegal or intrusive.
* Always follow legal and ethical guidelines when researching online targets.

## 4. Key Takeaways

* HTTrack is used to clone websites for offline viewing and analysis.
* CMS Enumeration tools help detect what platform a website is running on and whether it's up to date.
* The OSINT Framework links you to powerful free tools for safe, public data gathering.
* These tools are best for passive reconnaissance — no direct interaction or attacks involved.
* Always use them responsibly and in authorized environments.