Day 4 – Ethical Hacking

**Topics Covered:**

1. Social Media Reconnaissance  
2. Username Enumeration using Sherlock  
3. Web Technology Fingerprinting  
 - Wappalyzer (Extension)  
 - BuiltWith (Online Tool)  
 - WhatWeb (Command Line Tool)

# 1. Social Media Reconnaissance

Social media reconnaissance is an essential phase of OSINT (Open Source Intelligence). Ethical hackers or penetration testers use publicly available platforms like LinkedIn, Facebook, and Twitter to gather information about the employees of a targeted organization.  
  
The primary goal is to extract details such as:  
- Full names of employees (especially freshers or interns)  
- Designations and departments  
- Social handles and user activity  
  
Google Dorks can be used to find relevant profiles, such as:  
 site:linkedin.com/in/ "org.com"  
  
This reveals publicly indexed LinkedIn profiles related to the target domain. Once identified, these profiles can be further investigated using automated tools like Sherlock.

# 2. Sherlock – Username Enumeration Tool

Sherlock is a powerful and lightweight command-line tool that checks for the existence of usernames across hundreds of social media and public platforms. It helps ethical hackers collect the online footprint of individuals.  
  
🔹 Purpose:  
To locate an individual's presence across platforms like GitHub, Facebook, Twitter, Reddit, and more.  
  
🔹 Quick Installation (Kali Linux):  
Simply type the command below in Kali's terminal:  
 sherlock  
  
If Sherlock is not pre-installed, Kali will prompt with an install suggestion:  
 sudo apt install sherlock  
  
🔹 Manual GitHub Installation (Advanced Option):  
 git clone https://github.com/sherlock-project/sherlock.git  
 cd sherlock  
 pip3 install -r requirements.txt  
  
🔹 Usage:  
 sherlock employee\_name  
  
Sherlock will return links where the username exists, aiding in further profiling.

# 3. Web Technology Fingerprinting

Web fingerprinting is the process of detecting the technologies and platforms used to build a website. Understanding the tech stack helps penetration testers identify known vulnerabilities, outdated components, and potential entry points.  
  
Below are three primary tools used for fingerprinting:

## A. Wappalyzer (Browser Extension)

Wappalyzer is a browser extension that detects technologies used on websites in real time. It shows the CMS, JavaScript libraries, web frameworks, analytics tools, and more.  
  
🛠 How to use:  
1. Install from your browser's extension store.  
2. Visit the target website (e.g., https://org.com).  
3. Click the Wappalyzer icon to view the technology stack in use.

## B. BuiltWith (Online Tool)

BuiltWith is a powerful web-based tool that provides a comprehensive breakdown of a website’s backend and frontend technologies, including:  
- CMS (e.g., WordPress)  
- Web servers (Apache, Nginx)  
- Email and CDN services  
- SSL certificates and security details  
  
🛠 How to use:  
1. Go to https://builtwith.com  
2. Enter the domain name (e.g., org.com)  
3. Review the full technical stack report

## C. WhatWeb (Command Line Tool)

WhatWeb is a command-line web scanner used to identify what technologies a website is using, including server headers, CMS details, IP address, and more.  
  
🛠 Installation:  
 sudo apt install whatweb  
  
🛠 Usage:  
 whatweb org.com  
  
Example Output:  
 http://org.com [200 OK] Country[US], HTTPServer[Apache], X-Powered-By[PHP/7.4.3], Title[Org Official Website], Google Analytics

# Summary Table – Tools Overview

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Purpose** | **Platform** | **Command / URL** |
| Sherlock | Username enumeration | CLI (Kali) | sherlock employee\_name |
| Wappalyzer | Tech stack detection | Browser Extension | Use browser > Wappalyzer |
| BuiltWith | Web tech profiling | Online Tool | https://builtwith.com |
| WhatWeb | Web server + CMS detection | CLI (Kali) | whatweb org.com |

# Final Notes

- Social media recon helps in identifying targets for phishing and impersonation attacks.  
  
- Sherlock is a fast and accurate tool for enumerating usernames across online platforms.  
  
- Web fingerprinting tools like Wappalyzer, BuiltWith, and WhatWeb are essential for mapping the technical surface of a target.  
  
- Combine human and technical data to perform efficient ethical hacking during the reconnaissance phase.