Day 137

Topic: Footprinting & Reconnaissance

Objective: To gather as much information as possible about a target using passive and active techniques.

Theoretical Concepts:
Footprinting is the pre-attack phase. We learned about Passive Reconnaissance (gathering info without touching the target's server) vs. Active Reconnaissance. We discussed utilizing search engines, social media, and public records (Whois) to build a profile of the target organization.

Practical Work:
We used **Google Dorks** (advanced search queries) to find exposed files and login pages (e.g., *site:example.com filetype:pdf*). We used **Netcraft** to identify the technologies running on a website. We used the **Wappalyzer** browser extension to detect CMS versions, web servers, and frameworks used by target sites. We also performed Whois lookups to find domain registrar details.

Tools Used: Google Dorks, Netcraft, Wappalyzer, Whois.

Outcome: Ability to build a comprehensive information profile of a target before launching any direct scans.