Penetration Testing Phases and Key Terms

I. Reconnaissance and Information Gathering

- The initial phase involves collecting public information about the target.
- **Open-Source Intelligence (OSINT)** uses publicly available sources.
- Techniques include **Web Scraping**, **Google Dorking**, and social media profiling.
- Tools used: host, nslookup, dig, whois, knockpy, netdiscover, traceroute, whatweb, theHarvester, sherlock, wfw00f, Google Dorking, and the famous OSINT framework.

II. Scanning and Vulnerability Analysis

- Discovers open ports, services, OS versions, and other system information.
- Identifies potential vulnerabilities and misconfigurations.
- Involves active information gathering, directly interacting with the target.
- Tools used: nmap, searchsploit, nessus, OpenVAS, and MSF.

III. Exploitation and Gaining Access

- Exploits identified weaknesses to gain unauthorized entry.
- Methods include exploiting vulnerabilities, default configurations, brute-forcing, and social engineering.
- Tools used: **MSF**, **Exploit DB**, **Burp Suite**, **SQLmap**, **BeEF**, **Social Engineering Toolkit**, **Cobalt Strike**, and **PowerSploit**.

IV. Key Terms Defined

- **Vulnerability**: A weakness exploitable to compromise **CIA Triad**.
- **Malware**: Harmful self-contained executable needing user execution.
- **Exploit**: Code that leverages a vulnerability for unauthorized access.
- **Shellcode**: Small code to spawn a shell or execute commands.
- **Payload**: Code delivered via exploit to perform specific actions.