Day 12

Topic: Vulnerability Assessment

Objective: To identify and quantify security vulnerabilities in the system environment.

Theoretical Concepts:
We distinguished between Vulnerability Assessment (identifying flaws) and Penetration Testing (exploiting flaws). We discussed the Common Vulnerability Scoring System (CVSS) and how to prioritize patches. We introduced the concept of CVEs (Common Vulnerabilities and Exposures).

Practical Work:
We used the Nmap Scripting Engine (NSE) with the *--script vuln* flag to check for known vulnerabilities automatically. We also set up and ran **OWASP ZAP** (Zed Attack Proxy) to scan a web application for common flaws like missing headers and outdated components. We generated a report and analyzed the "High" and "Critical" severity findings.

Tools Used: Nmap (NSE), OWASP ZAP.

Outcome: Ability to run automated vulnerability scans and interpret the resulting security reports.