**3.3 Technology Stack**

**Tools explored :-**

1. **Nessus** – Used for automated **vulnerability assessment**, Nessus helps identify system misconfigurations, outdated software, and exploitable security weaknesses. It provides detailed reports categorizing vulnerabilities by severity.
2. **OWASP ZAP (Zed Attack Proxy)** – A widely used **penetration testing tool** for detecting vulnerabilities in web applications, including SQL Injection, Cross-Site Scripting (XSS), and broken authentication mechanisms.
3. **Burp Suite** – A powerful **web security testing tool** that allows security professionals to analyze and manipulate web traffic for identifying application vulnerabilities.
4. **Wireshark** – A **network packet analyzer** used for monitoring network traffic, detecting anomalies, and analyzing cyberattacks such as MITM (Man-in-the-Middle) attacks.
5. **Metasploit Framework** – A **penetration testing tool** that enables ethical hackers to exploit known vulnerabilities and assess an organization’s security posture.

**Kali Linux** – A **penetration testing and ethical hacking operating system** that includes numerous security testing tools such as Nmap, Hydra, and John the Ripper.