Technology Stack

To effectively analyze cybersecurity threats and implement security solutions, various tools and technologies are utilized in this project. These tools support vulnerability assessment, penetration testing, network monitoring, and real-time threat detection.

Tool Name	Category	Purpose
Kali Linux	Penetration Testing OS	Equipped with tools for ethical hacking and security testing.
Wireshark	Network Monitoring	Analyzes network packets to detect suspicious activities.
Nmap	Network Scanning	Discovers hosts and services in a network.
Metasploit	Penetration Testing	Identifies and exploits vulnerabilities.
Burp Suite	Web Security Testing	Detects SQL Injection and XSS vulnerabilities.
Snort	Intrusion Detection	Monitors network traffic for malicious activities.
OWASP ZAP	Web Application Security	Finds security flaws in web applications.
Hashcat	Password Cracking	Tests password strength using brute-force techniques.
Nessus	Vulnerability Assessment	Scans for known security issues in systems.

Splunk	SIEM	Analyzes security logs and detects threats in real time.

By utilizing these tools, the project enhances cybersecurity defenses and identifies security weaknesses effectively.