## 3.3 Technology Stack

### 3.3.1 TOOLS EXPLORED IN THIS PROJECT:

#### 1. OSINT (Open-Source Intelligence) Tools

| Tool Name | Use Case |
|---|---|
| Shodan | Scanning internet-connected devices, servers, and vulnerabilities |
| Maltego | Mapping relationships between domains, emails, IPs, and social networks |
| theHarvester | Gathering emails, subdomains, and IP addresses from OSINT sources |
| SpiderFoot | Automated OSINT for data gathering and reconnaissance |
| Amass | Subdomain enumeration and asset discovery |
| Recon-ng | Automating OSINT reconnaissance with modular functionality |
| WHOIS Lookup | Checking domain ownership and registration details |

#### 2.Threat Intelligence Platforms (TIPs)

| Tool Name | Use Case |
|---|---|
| MITRE ATT&CK | Cyber threat framework mapping attacker tactics and techniques |
| AlienVault OTX | Community-driven threat intelligence sharing |
| IBM X-Force Exchange | Threat intelligence feeds and research |
| VirusTotal | Analyzing suspicious files and URLs for malware detection |
| ThreatConnect | Advanced threat intelligence platform |
| Recorded Future | AI-powered threat intelligence and risk analysis |

#### 3. Network Scanning & Security Assessment Tools

| Tool Name | Use Case |
|---|---|
| Nmap (Network Mapper) | Scanning network hosts, services, and vulnerabilities |
| Wireshark | Network packet analysis for intrusion detection |
| Angry IP Scanner | Fast network scanning for IP discovery |
| OpenVAS | Comprehensive vulnerability scanning and reporting |
| QualysGuard | Cloud-based vulnerability assessment |

## 4. Web Application Security Tools

| Tool Name | Use Case |
|---|---|
| Burp Suite | Web vulnerability scanning and penetration testing |
| OWASP ZAP (Zed Attack Proxy) | Web application security testing |
| Nikto | Web server scanning for misconfigurations and vulnerabilities |
| SQLmap | Automated SQL Injection testing |
| W3af | Web application vulnerability scanning |

## 5.Penetration Testing & Exploitation Tools

| Tool Name | Use Case |
|---|---|
| Metasploit Framework | Automated penetration testing and exploit execution |
| Cobalt Strike | Adversary simulation and red teaming |
| ExploitDB | Database of known exploits for various applications |
| Hydra | Brute-force password cracking |
| John the Ripper | Password cracking for security testing |

## 6.Security Information & Event Management (SIEM) Tools

| Tool Name | Use Case |
|---|---|
| Splunk | Security log analysis and real-time monitoring |
| IBM QRadar | AI-driven threat detection and log analysis |
| Elastic SIEM | Open-source SIEM with real-time threat detection |
| ArcSight | Security event correlation and analysis |