Security Assessment Plan

1Environment & Initial Assessment

- □ Review system architecture, network topology, and firewall configurations.
- □ Validate Docker and VM configurations for Red/Blue team scenarios.
- □ Assess access control mechanisms, including SSO implementation.

2OSINT & Reconnaissance

- □ Conduct Open-Source Intelligence (OSINT) to identify external threats.
- □ Perform network scanning (e.g., Nmap, Shodan) to detect exposed services.
- □ Enumerate assets and gather intelligence for further testing.

3Web Application & Infrastructure Security Testing

- □ Perform vulnerability assessment and penetration testing on web applications.
- □ Analyze authentication mechanisms, including SSO misconfigurations.
- □ Simulate attack scenarios such as SQL Injection, XSS, and privilege escalation.

4Security Monitoring & Threat Detection

- □ Deploy and configure monitoring tools (e.g., Wazuh, Sysinternals) for real-time analysis.
- □ Set up log monitoring and threat detection mechanisms.
- □ Identify and document any anomalous activity.

5Reporting & Documentation

- □ Document findings, exploited vulnerabilities, and remediation steps.

□ Maintain a structured GitHub repository for documentation.

□ Deliver a comprehensive security playbook for implementation.