**Work Breakdown Structure (WBS)**

**Level 1: Project Management**

1.1 Project Initiation  
1.2 Stakeholder Engagement  
1.3 Project Planning & Scheduling  
1.4 Resource Allocation  
1.5 Team Collaboration Setup (GitHub, Jira)  
1.6 Project Closure & Reporting

**Level 2: Risk Assessment Phase**

2.1 Asset Identification & Inventory  
2.2 Threat Modeling & Attack Surface Mapping  
2.3 Vulnerability Scanning (Nessus, OpenVAS)  
2.4 Penetration Testing (Web/App/Network)

**Level 3: Risk Analysis & Prioritization**

3.1 Risk Categorization (High/Medium/Low)  
3.2 Impact Assessment  
3.3 Likelihood Assessment  
3.4 CVSS Scoring and Risk Matrix Development  
3.5 Approval of Top Risk List

**Level 4: Mitigation Strategy Implementation**

4.1 Control Design (Firewall, IDS/IPS, MFA, Encryption)  
4.2 Control Deployment and Configuration  
4.3 Incident Response Planning  
4.4 Security Policy Updates  
4.5 Change Management Logging (Jira)

**Level 5: Monitoring and Review**

5.1 SIEM Tool Integration (e.g., Splunk/Wazuh)  
5.2 Log Management and Alerts  
5.3 Security Metrics Dashboard  
5.4 Audit Trail Review  
5.5 Final Risk Evaluation and Adjustments

**Level 6: Documentation and Presentation**

6.1 Risk Assessment Report Compilation  
6.2 Mitigation Strategy Report  
6.3 Final Presentation Preparation