Aegis-Lite Project Blueprint: Phase 1 Development Strategy

Ethical Attack Surface Intelligence for SMEs

Hybrid CLI + Streamlit • Academic Excellence • 14-Week Implementation

---

Executive Summary

Aegis-Lite addresses a critical cybersecurity gap facing small and medium enterprises through an innovative, ethical, and accessible attack surface intelligence platform. Built as a comprehensive academic project, it transforms complex security reconnaissance into a streamlined, user-friendly experience that delivers actionable insights within minutes rather than days.

The project demonstrates exceptional alignment with academic objectives while solving real-world problems, positioning students to develop industry-relevant skills through hands-on implementation of modern cybersecurity tools and methodologies.

Problem Statement & Market Context

The SME Cybersecurity Challenge

Small and medium enterprises face an increasingly complex digital threat landscape, with 68% of security breaches occurring through unknown or poorly monitored digital assets. Traditional enterprise security solutions present significant barriers:

- **Cost Prohibitive**: Commercial attack surface management tools typically cost $20,000+ annually
- **Complexity Barrier**: Manual tool integration requires 2+ days of setup and specialized expertise
- **False Positive Overload**: Generic scanning tools generate overwhelming numbers of irrelevant alerts
- **Resource Constraints**: SMEs lack dedicated security personnel to manage complex toolchains

The Aegis-Lite Solution

Aegis-Lite transforms this paradigm by delivering enterprise-grade security intelligence through an elegant, unified interface. The platform provides:

Rapid Deployment: Single Docker command execution with complete environment setup
Intelligent Scanning: Automated asset discovery with ethical rate limiting and resource management
Actionable Intelligence: Trust scoring algorithms that prioritize findings based on actual risk
Compliance Ready: Professional PDF reports suitable for regulatory requirements

The solution bridges the gap between academic learning and professional application, providing students with deep technical experience while creating tangible value for the cybersecurity community.

Technical Architecture & Implementation Strategy

Core Technology Stack

Our technology selection balances academic accessibility with professional-grade capabilities:

Foundation Layer

- **Python 3.10**: Provides robust ecosystem integration and student-friendly development environment
- **Click Framework**: Enables intuitive command-line interface design with comprehensive help systems
- **SQLite Database**: Lightweight persistence layer requiring no external dependencies

Discovery & Scanning Engine

- **Subfinder**: Ethical subdomain enumeration with built-in rate limiting
- **HTTPX**: High-performance HTTP client for service discovery and validation
- **Nuclei**: Focused vulnerability detection using curated template selection

User Experience Layer

- **Streamlit**: Rapid prototyping platform for interactive dashboard development
- **ReportLab**: Professional PDF generation for compliance documentation
- **Docker**: Containerization for consistent deployment across environments

Quality Assurance

- **pytest**: Comprehensive testing framework with coverage analysis
- **Selenium**: Automated UI testing for dashboard validation
- **psutil**: Resource monitoring for ethical operation compliance

System Architecture Philosophy

The architecture emphasizes modularity, ethical operation, and educational value through clear separation of concerns:

Discovery Module: Handles asset enumeration with strict rate limiting and robots.txt compliance
Scanning Module: Coordinates vulnerability detection with configurable template selection
Scoring Module: Implements trust algorithms based on security posture indicators
Reporting Module: Generates professional documentation with actionable recommendations

---

Academic Alignment & Learning Outcomes

Comprehensive Course Outcome Mapping

The project meticulously addresses all academic requirements while providing practical industry experience:

CO1 - Real-World Problem Identification: Direct engagement with SME cybersecurity challenges through stakeholder interviews and market research

CO2 - Requirements Engineering: Systematic gathering of user needs through structured interviews and use case analysis

CO3 - Agile Development Methodology: Full Scrum implementation with sprint planning, daily standups, and retrospectives documented in comprehensive Scrum Book

CO4 - System Analysis & Design: Complete architectural documentation including entity-relationship diagrams, user interface wireframes, and detailed system specifications

CO5 - Testing Strategy: Test-driven development approach with >85% code coverage, automated UI testing, and comprehensive integration validation

CO6 - Module Integration: Sophisticated coordination of multiple scanning tools through unified Python orchestration layer

CO7 - Documentation & Deployment: Professional LaTeX report, demonstration video, and containerized deployment to Docker Hub

Skill Development Framework

Students gain expertise across multiple domains:

Technical Skills: Python development, database design, containerization, CI/CD pipeline implementation
Security Skills: Vulnerability assessment, ethical hacking principles, compliance reporting
Professional Skills: Agile methodologies, technical writing, presentation delivery
Industry Tools: Docker, Git, testing frameworks, documentation systems

---

Implementation Timeline & Milestones

Phase 1: Foundation (Weeks 1-4)

Project Initialization

- Team formation and role assignment
- Git repository establishment with initial commit structure
- Comprehensive synopsis development addressing problem scope and solution approach
- Mock SME interviews with classmates to validate requirements
- Development environment setup including all required tools and dependencies

Core CLI Development

- SQLite database schema design for asset storage and scan results

- Implementation of basic discovery commands using Subfinder integration
- HTTPX integration for port scanning and service enumeration
- Ethical scanning guidelines implementation with rate limiting
- Initial unit test development achieving 30% code coverage

Phase 2: Core Functionality (Weeks 5-8)

Advanced Scanning Capabilities

- Nuclei integration with carefully selected vulnerability templates
- Trust scoring algorithm development based on security indicators
- Comprehensive scan result storage and retrieval system
- Ethical compliance monitoring with resource usage tracking
- Test coverage expansion to 50% with integration testing

User Interface Development

- Streamlit dashboard creation with three primary tabs: Scan, Results, Report
- Real-time monitoring integration using psutil for resource management
- Interactive asset tables with vulnerability display
- Live scan progress tracking with ethical compliance indicators
- Selenium-based UI testing framework implementation

Phase 3: Integration & Enhancement (Weeks 9-12)

Reporting & Containerization

- Professional PDF report generation using ReportLab
- Comprehensive Docker containerization of entire application stack
- Docker Hub image publication with automated build pipeline
- Trust radial chart visualization for enhanced dashboard impact
- CI/CD pipeline implementation for automated testing and deployment

Quality Assurance & Optimization

- Comprehensive edge case testing and performance validation
- Resource monitoring and optimization for student hardware constraints
- Trust scoring algorithm refinement incorporating vulnerability severity
- User experience polish with comprehensive internal review process
- Achievement of >85% overall test coverage with detailed reporting

Phase 4: Finalization & Submission (Weeks 13-14)

Documentation & Presentation

- Comprehensive LaTeX report covering all project aspects
- Professional demonstration video highlighting key capabilities
- Final stakeholder feedback collection and integration
- Presentation slide deck preparation with visual impact optimization
- Complete codebase and documentation submission to GitHub

Optional Enhancement: MITRE ATT&CK framework integration for vulnerability mapping and industry-standard threat categorization

---

Ethical Framework & Compliance

Responsible Security Research

Aegis-Lite operates under strict ethical guidelines that ensure responsible security research:

Rate Limiting: All scanning operations include mandatory delays to prevent service disruption
Robots.txt Compliance: Automatic respect for website crawling restrictions
Resource Monitoring: Real-time CPU and memory usage tracking with automatic cutoffs
Scope Limitation: Maximum asset limits prevent overwhelming target infrastructure

GDPR & Privacy Considerations

The platform implements privacy-by-design principles:

- No personal data collection without explicit consent
- Clear disclaimers regarding data handling practices
- Automatic anonymization of sensitive information in reports
- User-controlled data retention policies

Hardware Resource Management

Critical safeguards ensure stable operation on student hardware:

- **Asset Limitation**: Maximum 50 assets per scan to prevent system overload
- **Thread Management**: CPU core-matched threading prevents resource exhaustion
- **Memory Monitoring**: Automatic scan pausing when memory usage exceeds 75%
- **Scan Delays**: 2-second intervals between requests for ethical operation

---

Future Expansion Strategy

Phase 2 Advanced Capabilities

Artificial Intelligence Integration

- Machine learning-based vulnerability prioritization using SHAP explainability
- Automated false positive reduction through intelligent filtering
- Risk prediction modeling based on historical scan data

Cloud Infrastructure Scaling

- AWS-based architecture supporting 10,000+ asset scanning
- Multi-tenant capabilities for service provider deployment
- Terraform-based infrastructure as code implementation

Advanced Threat Intelligence

- Dark web monitoring for exposed credentials and data
- Threat intelligence feed integration for enhanced context
- Automated alerting for critical security events

Mobile Platform Extension

- React Native application for on-the-go scan management
- Push notification system for critical vulnerability alerts
- Mobile-optimized reporting and dashboard interfaces

Enterprise Feature Set

Enhanced Scanning Capabilities

- OpenVAS integration for comprehensive network vulnerability assessment
- OWASP ZAP integration for advanced web application security testing
- Authenticated scanning for internal asset assessment

Advanced Reporting & Analytics

- Executive dashboard with risk trend analysis
- Compliance mapping for multiple regulatory frameworks
- Automated remediation guidance and prioritization

Success Metrics & Evaluation Criteria

Technical Performance Indicators

Scanning Efficiency: Complete asset discovery and vulnerability assessment in <5 minutes
Accuracy Standards: Trust score accuracy >80% with false positive rate <20%
Resource Optimization: Stable operation on student hardware with <75% resource utilization
Code Quality: >85% test coverage with comprehensive documentation

Academic Achievement Metrics

Course Outcome Compliance: Full mapping and demonstration of all CO requirements
Documentation Quality: Professional LaTeX report with comprehensive technical detail
Presentation Excellence: Compelling demonstration with clear value proposition
Industry Relevance: Stakeholder feedback confirming real-world applicability

Impact Assessment

Educational Value: Deep technical skill development across multiple domains
Community Benefit: Enhanced cybersecurity posture for vulnerable SME population
Career Preparation: Industry-relevant experience with modern security tools
Innovation Potential: Foundation for advanced research and commercial development

---

Risk Management & Mitigation Strategies

Technical Risk Factors

Tool Integration Complexity: Mitigated through modular architecture and comprehensive testing
Resource Constraints: Addressed through strict hardware safeguards and optimization
False Positive Management: Reduced through careful template selection and trust scoring
Ethical Compliance: Ensured through built-in rate limiting and monitoring systems

Academic Risk Factors

Scope Creep: Managed through clear milestone definition and regular progress review
Timeline Pressure: Addressed through realistic task estimation and buffer allocation
Technical Difficulty: Mitigated through mentor support and incremental development
Documentation Burden: Streamlined through continuous documentation practices

Mitigation Strategies

Weekly Progress Reviews: Regular assessment of milestone achievement and risk factors
Mentor Engagement: Proactive consultation for technical challenges and guidance
Peer Collaboration: Cross-team knowledge sharing and problem-solving support
Contingency Planning: Alternative approaches for critical path dependencies

---

Conclusion

Aegis-Lite represents a sophisticated fusion of academic rigor and professional application, delivering tangible value to the cybersecurity community while providing students with comprehensive technical experience. The project demonstrates exceptional potential for both educational achievement and real-world impact.

Through careful balance of ambitious objectives and realistic constraints, the 14-week implementation plan provides a clear pathway to success. The ethical framework ensures responsible development practices, while the modular architecture supports both immediate academic goals and long-term expansion opportunities.

The comprehensive documentation and presentation strategy positions the project for maximum impact, providing clear evidence of learning achievement and professional readiness. By addressing genuine market needs through innovative technical solutions, Aegis-Lite exemplifies the highest standards of academic project development.

This blueprint serves as both a detailed implementation guide and a demonstration of the project's exceptional potential for contributing to cybersecurity education and SME security enhancement. The careful integration of technical excellence, ethical responsibility, and educational value creates a foundation for sustained success and meaningful impact.