Aegis-Lite: Ethical Attack Surface Intelligence for SMEs

Abstract

Aegis-Lite is a free, automated cybersecurity tool designed for SMEs. It discovers hidden digital assets, scans for vulnerabilities, and generates actionable trust scores in under 5 minutes through both CLI and web interfaces, addressing the critical gap in affordable security intelligence.

Problem

SMEs face 68% of breaches through unknown assets (forgotten subdomains, misconfigured servers). Commercial solutions cost $20K+ annually, manual tool chains require 2+ days setup with specialized expertise, and existing scanners generate overwhelming false positives that small teams cannot process effectively.

Existing Solutions

- **Commercial**: Shodan, Censys, RiskIQ ($20K+/year, enterprise-focused)
- **Manual**: Subfinder + Nmap + Nuclei (complex integration, time-intensive)
- **Basic**: Nessus, OpenVAS (generic output, configuration complexity)
- **Gap**: No free, user-friendly, SME-tailored solution with integrated workflow

Proposed Solution

Aegis-Lite implements a modular Python architecture with four core components: Discovery Engine orchestrates Subfinder for passive subdomain enumeration and HTTPX for active service fingerprinting, storing results in SQLite with normalized asset schemas. Scanning Engine coordinates Nuclei template execution with configurable vulnerability detection, implementing thread pooling for performance while maintaining ethical rate limits. Intelligence Engine processes scan data through weighted trust algorithms considering HTTPS implementation, open port analysis, and CVE severity mappings. Reporting Engine generates multi-format outputs via ReportLab PDF generation and Streamlit real-time dashboards. The system employs psutil for resource monitoring, Docker multi-stage builds for deployment, and pytest-driven TDD for reliability.

Functionalities

Input: Target domain, ethical scan limits, output preferences
Process: Subfinder subdomain enumeration → HTTPX service discovery → Nuclei vulnerability scanning → trust algorithm processing → report generation
Output: Comprehensive asset inventory, prioritized vulnerability reports, interactive dashboard, professional PDF documentation

Technical Stack

- **Core**: Python 3.10, Click (CLI), Streamlit (UI), SQLite (database)
- **Security**: Subfinder, HTTPX, Nuclei templates, psutil monitoring
- **Infrastructure**: Docker containerization, ReportLab PDF generation, pytest testing

Key Features

- **Ethical Scanning**: Built-in rate limiting, robots.txt compliance, resource monitoring
- **Trust Scoring**: 0-100 risk assessment algorithm prioritizing critical vulnerabilities
- **Dual Interface**: CLI commands for automation, Streamlit dashboard for visualization
- **Professional Reports**: PDF generation with compliance-ready documentation
- **Docker Deployment**: Single command containerized setup with all dependencies
- **Resource Management**: Hardware-aware limits (max 50 assets, 75% memory cutoff)
- **Comprehensive Testing**: >85% code coverage with automated UI/integration tests

Future Expansion

Phase 2 (If Time Permits):

- AI-powered vulnerability triage using machine learning
- MITRE ATT&CK framework integration for threat mapping
- Trust radial charts for enhanced dashboard visualization
- OWASP ZAP integration for authenticated web application scanning

Long-term Vision:

- Cloud scaling with AWS/Terraform for enterprise deployment
- Dark web monitoring for exposed credentials
- Mobile app development with React Native
- Advanced threat intelligence feed integration

Deliverables

- Complete source code repository (GitHub)
- Academic LaTeX report (15 pages)
- Professional demo video (5 minutes)
- Production Docker Hub image
- Comprehensive test suite with documentation