Project Abstract: Automated Reconnaissance Orchestrator (Phase 1)

Problem:

Cybersecurity professionals spend hours manually running different security tools to assess website vulnerabilities. Each tool must be executed separately, results copied manually, and findings compiled into reports - a process prone to errors and time waste.

Solution:

ARO combines six popular security tools into one automated system:

1. **Input:** Website domain (e.g., `example.com`)
2. **Automated Process:**
   - Finds all subdomains and related websites
   - Checks which sites are actually running
   - Discovers hidden web pages and files
   - Scans for known security vulnerabilities
3. **Output:** Professional PDF report with all findings

Technology:

Built using Python for automation, Docker for easy deployment, and follows industry-standard development practices including version control and automated testing.

Key Benefits:

Replaces 4-6 hours of manual work with a single command that completes in minutes. Reduces human errors while producing consistent, professional reports. Meets all academic project requirements including documentation and proper software engineering practices.

Impact:

Makes professional security testing accessible to students and small businesses. Creates foundation for advanced AI-powered features in future development phases.

(149 words)