ASM-Lite: Abstract

Project Title: Ethical Attack Surface Discovery Tool with Trust Scoring

Problem Solved: Small businesses face cyber threats from shadow IT and forgotten internet infrastructure (old subdomains, abandoned servers, forgotten APIs). These hidden assets create security blind spots but existing discovery tools are either too expensive or produce too many false alarms that overwhelm small security teams.

Solution: An open-source tool that helps companies find their hidden internet-facing assets:

1. **Input:** Company domain name (e.g., startup.com)
2. **Discovery Process:**
   - Searches public certificate records and DNS databases
   - Finds subdomains and checks for open services
   - Follows ethical scanning rules (respects robots.txt, uses rate limits)
3. **Trust Scoring:**
   - Cross-checks findings across multiple data sources
   - Assigns confidence scores (0-100%) to each discovered asset
   - Filters out false positives to reduce noise
4. **Output:** Clean reports showing verified assets, what's exposed, and risk levels

Technical Implementation: Python-based tool with database storage, command-line interface, and Docker packaging for easy deployment.

Impact: Gives small businesses affordable visibility into their shadow IT infrastructure, helping them secure forgotten assets before attackers find them. Reduces breach risks through automated discovery while maintaining ethical standards.