Project Abstract: Ethical Attack Surface Discovery Tool w/Trust Scoring (Phase 1)

Problem Solved:

Cyber threats against small businesses posed by shadow IT and forgotten internet infrastructure (old subdomains, abandoned servers, forgotten APIs). These hidden assets create security blind spots but current discovery tools are either too costly or generate too many false positives that overwhelm small security teams.

Solution:

An open-source tool that assists businesses in discovering their hidden internet-facing assets: **1.**

Input: Company domain name (example: startup.com)

2. Discovery Process:

- Queries public certificate records and DNS stores
- Locates subdomains and searches for open services
- Adheres to ethical scanning guidelines (honors robots.txt, employs rate limits)

3. Trust Scoring:

- Verifies results across multiple data sources
- Assigns confidence scores (0-100%) to each found asset
- Eliminates false positives to minimize noise

4. Output: Clean reports indicating verified assets, what's exposed, and risk levels

Technical Implementation: Command-line tool based on Python with database storage, commandline interface, and Docker packaging for convenient deployment.

Impact: Provides small companies with low-cost visibility into their shadow IT infrastructure so that they can secure overlooked assets before attackers do. Mitigates breach risks with automated discovery without violating ethical standards.