



🔗 Software Specification Document

Title: Automated Cybersecurity Lead Scanner for Insurance Risk Assessment

Purpose To automate the scanning and risk evaluation process for potential clients (leads) of a cybersecurity insurance company. Each lead is a domain representing a company. The software will discover publicly exposed services, scan open ports, assess vulnerabilities, and assign a security risk score.

Key Components

1. Lead Input Module

- **Input Methods:**
 - CSV or JSON file upload
 - REST API for ingestion
- **Input Fields:**
 - Domain (FQDN)
 - Company Name
 - Timestamp
- **Validation:**
 - Ensure domain format is valid
 - Remove duplicate entries

2. Asset Discovery Module

- **Functions:**
 - DNS Enumeration: A, AAAA, CNAME, MX, TXT, NS
 - Subdomain Discovery: Tools like `subfinder`, `Amass`, or `crt.sh`
 - HTTP(S) Probing: Detect accessible endpoints and categorize (website, admin panel, VPN login, etc.)
- **Output:**
 - List of assets with metadata (protocol, IP, port, detected tech stack, title)

3. Port Scanning Module

- **Tools:**
 - `Nmap`, `Masscan`
- **Scan Capabilities:**
 - TCP SYN Scan
 - Optional: UDP scan
 - Service Detection (`-sV`)
 - OS Detection (`-O`)
- **Output:**
 - Open ports with protocol and service version

4. Vulnerability Assessment Module

- **Tools/Methods:**
 - CVE Matching via `nuclei`, `OpenVAS`, or online CVE APIs
 - Vulnerability lookup based on version signatures
- **Output:**
 - CVE list with severity (CVSS score)
 - Associated ports/services
 - Indicators of exploitability

5. Risk Scoring Engine


- **Scoring Metrics:**
 - Number and type of exposed services
 - Presence of high-risk open ports (e.g., 3389, 21, 23)
 - Known vulnerabilities with high severity
 - Misconfigured SSL/TLS certificates
- **Output:**
 - Final risk score (0-100)
 - Risk category (Low, Medium, High, Critical)

6. Dashboard & Reporting (Optional for MVP)

- **UI Components:**
 - Searchable and sortable table views
 - Domain-wise summary
- **Export Formats:**
 - PDF, Excel, JSON
- **Reports Include:**
 - Summary of findings
 - Visual risk indicators
 - Full scan history

Integrations - REST API for sending results to external systems (CRM, SIEM, risk platform) - Email alerts on detection of critical vulnerabilities

⚠ **Security & Compliance** - Rate limiting and scanning ethics (avoid denial-of-service) - Use only authorized domains - Encrypt scan results at rest - Implement audit logging for all scans

 **MVP Scope** - Lead ingestion via CSV/API - Asset and subdomain discovery - Port scanning using `Nmap` - Basic vulnerability matching with public CVE data - Risk scoring engine

Version: 1.0

Date: June 2025

Owner: Cybersecurity Insurance Tech Team