K.R. MANGALAM UNIVERSITY

THE COMPLETE WORLD OF EDUCATION

Sentinel-X: A Comprehensive Cybersecurity Toolkit

Project Supervisor: Ruchika Bhakar
Course Code: ENSI152
Group: Y1-2024-25-G206

Team Members:

- Akansh Pandey (240183006) – Chatting App and Frontend Developer
- Akshaya Tanwar (2401840006) – Vulnerability Scanner Developer
- Kartikey (2401720014) – Port Scanner Developer
- Palak Kashyap (2401840007) – Password Strength Checker Developer

Introduction

The increasing dependency on digital communication and online systems has led to a surge in cyber threats such as data breaches, ransomware, and unauthorized intrusions. Traditional security mechanisms are often static and lack adaptability to real-time threats. **Sentinel-X** is developed as a solution to this problem by combining secure real-time communication with a suite of cybersecurity tools, including a password strength checker, vulnerability scanner, and port scanner—all integrated into a unified, user-friendly toolkit.

Significance of Comprehensive Cybersecurity

Sentinel-X ensures proactive defense by offering:

- **Real-Time Adaptability** to counter evolving cyber threats.
- **Scalability** across different environments from individual to enterprise levels.
- **User Control** with customizable settings and full visibility.
- **Advanced Technologies**, including AES encryption, real-time monitoring, and automated analysis.

Literature Review

Research reveals the limitations of existing cybersecurity tools:

- **Limited User-Controlled Encryption**: Proprietary encryption limits transparency.
- **Fragmented Toolsets**: Users must juggle between separate applications.
- **Lack of Real-Time Adaptability**: Static configurations can't respond to dynamic threats.
- **Low Transparency**: Users cannot audit or customize how data is secured.

Sentinel-X addresses these gaps with an integrated, open-source platform offering encryption, scanning, and user-driven customization.

Research Gaps

- **Fragmentation**: Lack of unified platforms.
- **Limited User Control**: Centralized encryption dominates the market.
- **Accessibility**: Tools are too technical for general users.
- **Adaptability**: Static systems can't react quickly to threats.
- **Transparency**: Proprietary tools offer no auditability.

Objectives

- Build a **secure chat system** with AES encryption.
- Provide tools for **vulnerability scanning** and **port scanning**.
- Develop a **password strength checker**.
- Offer **real-time adaptability** to detect evolving threats.
- Ensure full **user control** and **auditability**.
- Support **multi-client scalability**.
- Enable **custom security configurations**.
- Create a **user-friendly GUI**.

Modules Included

1. **Secure Chatting Application**
    - **Tech Stack**: Supabase, JavaScript, AES-GCM
    - **Features**:

        - End-to-end encrypted chat.
        - Typing indicators, friend search, and online status.
        - Hacker-themed responsive UI.
        - Supabase for authentication and real-time messaging.

2. **Vulnerability Scanner**
    - **Backend**: Flask, Python libraries (requests, beautifulsoup4)
    - **Frontend**: HTML/JS
    - **Capabilities**:
        - Crawling and link extraction.
        - Header checks, SQLi, and XSS detection.
        - Admin panel discovery.
        - Generates plain-text report.
3. **Port Scanner**
    - **Backend**: Flask, Python (socket)
    - **Frontend**: HTML/JS
    - **Features**:
        - Fast, threaded scanning of common ports.
        - Input-based targeting.
        - Real-time UI feedback.

        - Implements Flask APIs to interact with the frontend.

4. **Password Strength Checker** (In Progress)
    - **Tech Stack**: HaveIBeenPwned API, Regex, entropy-based methods
    - **Features**:
        - Analyzes password complexity.
        - Compares with breach patterns from the HaveIBeenPwned API.
        - Suggests improvements visually.

Methodology

1. **Requirements & Intelligence Gathering**
    - Use CVE databases, security advisories.
    - Identify attack vectors and user environments.
2. **System Architecture**
    - Develop a modular design using **Flask** and **Supabase**.
    - Integrate modules with a central web interface hosted on **Vercel** and **Render**.
3. **Implementation**
    - **Chat Encryption**: AES-256 with SHA-256 hashes for end-to-end encryption.
    - **Scanning**: Uses **requests**, **socket**, and **beautifulsoup4** for vulnerability and port scanning.
    - **Password Checks**: Uses **Regex** and entropy-based methods along with the **HaveIBeenPwned API** for breach checks.

4. **Simulation & Testing**
    - Unit testing for all modules.
    - Controlled environment simulations.
    - Real-time attack response scenarios to ensure proper adaptation to evolving threats.
5. **Performance Analysis**
    - Log scan activity, encryption throughput.
    - Benchmarking against other tools.
    - Gather user feedback for refinements.

Expected Outcomes

- A deployable, full-featured cybersecurity toolkit.
- Enhanced encryption, threat detection, and reporting capabilities.
- Visual dashboard for scan results, integrating **port scanner**, **vulnerability scanner**, and **password strength checker**.
- A modular, scalable, open-source solution that is adaptable to both individual users and enterprise-level systems.

Deployment Strategy

- **Frontend** (Vercel): HTML/JS files hosted under one domain for easy access.
- **Backend** (Render): **Flask** APIs for scanning accessed via **fetch()** requests.

- **Cross-Origin**: Enabled using **Flask-CORS** to allow the frontend and backend to communicate seamlessly across different domains.

Conclusion

Sentinel-X demonstrates a comprehensive approach to digital security through a unified platform. With **real-time encrypted chat**, **vulnerability and port scanners**, and a **password strength checker**, users gain full visibility and control over their cybersecurity posture. Its **open-source architecture** ensures transparency and future extensibility, making it both a **learning resource** and a **practical security toolkit** for various environments.