IP VULNERABILITY TRACKER

***A***

***Synopsis Report***

**BACHELOR OF TECHNOLOGY**

**in**

**COMPUTER SCIENCE & ENGINEERING**

***by***

|  |  |
| --- | --- |
| **Name** | **Roll No.** |
| **Shreyanshi Dobhal** | **R2142220656** |
| **Akshat Negi** | **R2142220414** |
| **Arush Dubey** | **R2142220314** |
| **Ameya Taneja** | **R214220** |

***under the guidance of***

**Prof. Akashdeep Bhardwaj**



**School of Computer Science**

**University of Petroleum & Energy Studies**

**Bidholi, Via Prem Nagar, Dehradun, Uttarakhand - 248001**

**(AUG-DEC 2024)**

**ABSTRACT**

This report presents a comprehensive analysis of Internet Protocol (IP) data, focusing on detecting and mitigating security threats within a network. The project leverages advanced algorithms to identify and classify IP traffic anomalies, with the aim of enhancing network security. By analysing sample IP data and employing a reference algorithm, the project aims to highlight vulnerabilities, mitigate risks, and improve overall network efficiency.

**INTRODUCTION**

With our growing hyper-connected world, our dependence on the Internet has increasingly grown, with innovation like e-commerce, fast communication. Each day, huge amounts of data travels through the globe. However, with this massive flow of personal and public data daily, there comes a very significant need to safeguard Data and Networks, from various Cyber Threats.

The growing dependence on the Internet and innovation have led to a significant need to safeguard data and networks from cyber threats. This project aims to analyze IP traffic data using advanced algorithms to identify potential security breaches. By combining real-time data analysis with automated threat response capabilities, the system provides a dependable defence against cyber-attacks. The project focuses on reliable and fast information about IP, enabling the scalability of large-scale networks. The goal is to deliver a comprehensive cybersecurity tool that provides comprehensive protection against cyber threats.

**PROBLEM STATEMENT**

Traditional IP analysis tools are severely limited in their capacity to identify and mitigate security threats in real time due to the complexity and size of modern networks. Due to these flaws, networks may be compromised and breaches may occur. Cybercriminals may take advantage of these vulnerabilities. This project is focused on creating a sophisticated IP vulnerability tracker framework in order to address this important problem. In order to provide a dependable and scalable defense against the ever-changing landscape of cyber risks, the system is built to provide accurate, real-time detection and response to security threats.

**SWOT ANALYSIS**

**Strengths**

* **Real-Time Threat Detection**: The system's ability to analyse IP traffic as it happens provides a powerful defence mechanism, allowing immediate identification and response to potential security threats. This real-time capability ensures that malicious activities, such as DDoS attacks or unauthorized access attempts, are detected and mitigated before they can cause significant damage.
* **Scalability**: Designed to handle vast amounts of data, vulnerability tracker system is highly scalable, making it suitable for large, complex networks with millions of IP connections. This adaptability ensures that the system remains effective as network demands grow, from small businesses to global enterprises.

**Weaknesses**

* **Resource-Intensive Processing**: The computational demands of real-time IP traffic analysis, especially in large-scale networks, can be significant. This may require substantial investment in hardware and computational resources, potentially limiting its accessibility to organizations with smaller IT budgets.

**Opportunities**

* **Integration with Existing Security Infrastructures**: The Vulnerability tracker system can be seamlessly integrated with other security tools like Geolocation. This integration offers a holistic approach to threat management, combining real-time detection with broader incident response capabilities.
* **Customization for Industry-Specific Needs**: The system can be tailored to meet the unique security requirements of different industries, such as finance, healthcare, and government. By customizing detection algorithms and thresholds, the system can provide targeted protection against industry-specific threats, increasing its value and relevance.

**Threats**

* **Evolving Cyber Threat Landscape**: The constantly changing nature of cyber threats poses a challenge to the effectiveness of this vulnerability tracker system. New attack techniques and vulnerabilities may emerge that the current algorithms and data models are not equipped to handle, necessitating continuous updates and adaptations.
* **Data Privacy and Regulatory Compliance**: Handling and analysing IP data, especially in regions with strict data protection laws, introduces potential privacy concerns. Ensuring compliance with regulations and other privacy frameworks is crucial to avoid legal repercussions and maintain user trust.

**Project Architecture**

The Vulnerabiliy Tracker project architecture is designed to deliver comprehensive insights into website security and performance by integrating multiple scanning tools and APIs. The system is built with a modular approach, ensuring scalability, reliability, and ease of integration with various external services.

1**. System Overview**

The system architecture consists of several key components:

* Frontend (ReactJS): The user interface is built with React, providing an interactive dashboard where users can view detailed insights about a website. This includes sections for IP information, SSL chain, DNS records, server location, open ports, and more.\
* Backend (Node.js/Express): The backend serves API requests from the frontend, processes data, and interacts with the database. It also handles communication with external APIs for additional data retrieval and analysis.
* Database (MongoDB): All collected data is stored in a MongoDB database. This includes historical data on IPs, DNS records, SSL certificates, and more, enabling the system to perform trend analysis and provide historical insights.
* External APIs:
  + Google Cloud API: Used to retrieve quality metrics for a website, enhancing the depth of analysis provided by the system.
  + Shodan API: This API provides information on associated hostnames for a given domain, which is crucial for identifying potential security risks.
  + WhoAPI: Offers comprehensive Whois records, providing detailed domain information that supports the identification of potential vulnerabilities.
* Scanning Modules: The system includes various scanning modules that perform specific checks and analyses:
  + IP Information: Retrieves and analyzes the IP address data of a given website.
  + SSL Chain: Examines SSL certificates to ensure they are valid and properly configured.
  + DNS Records: Collects and analyzes DNS records, including TXT and A records, to ensure proper configuration and security.
  + Open Ports: Scans for open ports on the server, which could be potential entry points for attackers.
  + HTTP Security Features: Analyzes HTTP headers and other configurations to assess the website’s security posture.
  + Site Performance and Carbon Footprint: Measures the website's performance metrics and evaluates its environmental impact based on energy consumption.

**2. Data Flow**

* Data Collection: The frontend sends a request to the backend to analyze a specific website. The backend orchestrates the scanning process by invoking the relevant scanning modules and external APIs.
* Data Processing: The results from the scanning modules and external APIs are processed and stored in the database. The backend also performs additional analysis, such as identifying trends or anomalies in the data.
* Data Presentation: The processed data is sent back to the frontend, where it is displayed on the dashboard. Users can view detailed information about the website’s security, performance, and environmental impact.

**3. API Configuration**

To enhance the system’s capabilities, the following environmental variables can be configured:

* GOOGLE\_CLOUD\_API\_KEY: For accessing Google Cloud’s site quality metrics.
* SHODAN\_API\_KEY: To retrieve associated hostnames via Shodan.
* WHO\_API\_KEY: For obtaining comprehensive Whois records.

Additional configuration settings include port assignments, API rate-limiting, CORS policies, and timeout limits, which ensure the system operates smoothly and securely in various environments.

4. **Future Enhancements**

In the future, we plan to integrate web vulnerability exploitation tools into the system, enabling us to actively test the resilience of websites against various hacking techniques. This addition will allow for comprehensive assessments of a site's defenses, providing deeper insights into its ability to withstand potential cyber-attacks.

**Algorithm**

The algorithms used in our project include:

1. **Merge Sort Algorithm**
   * **Usage:** Applied to sort data fetched from APIs and to organize packets by timestamp, size, or other criteria.
   * **Logic:** The algorithm divides the dataset into smaller segments, recursively sorts them, and then merges the sorted segments. It operates with a time complexity of O(n log n) and is suitable for large datasets. Merge sort is stable and can be parallelized for multi-threaded environments.
2. **Heap Sort Algorithm**
   * **Usage:** Utilized for managing and sorting dynamically updated data from network streams.
   * **Logic:** Builds a heap data structure, then repeatedly extracts the maximum element and rebuilds the heap. Heap sort maintains a time complexity of O(n log n) and performs sorting in place, making it efficient in terms of memory usage.

**System Design**

The system is designed to be both robust and adaptable, using a combination of APIs and a central database to gather and analyze detailed information about websites. This approach enables us to provide insights into various aspects, such as IP details, SSL chains, DNS records, and server configurations.

One of the key components of the system is its comprehensive dashboard, which serves as the main interface for users. The dashboard is structured to present the analyzed data clearly and accessibly, giving a thorough overview of a website’s security status. Users can track a variety of important metrics, including IP information, SSL chain integrity, DNS records, and open port status. Additionally, it offers insights into site performance, security settings, and potential vulnerabilities, making it a practical tool for both technical teams and decision-makers.

**Future Work**

Scalability is a central consideration, ensuring that the system can manage increased data loads as more websites are analyzed. It’s also built to integrate smoothly with other security tools, making it a flexible addition to any organization’s security setup. In the future, we plan to incorporate web vulnerability exploitation tools. This will allow the system to test how well websites hold up against potential hacks, offering deeper insights into their security resilience.

**Area of Application**

The IP analysis system provides crucial insights and protection across various sectors. Below are four key areas where the system can be effectively utilized:

1. **Corporate Network Security**
   * **Use:** The system continuously monitors enterprise networks for anomalies and potential security breaches, offering real-time analysis and threat detection.
   * **Helpfulness: It significantly enhances the protection of sensitive corporate data, ensures the integrity of business operations, and mitigates risks associated with cyber threats.**
2. **Financial Sector**
   * **Use:** The system monitors transaction networks and online banking platforms to detect and analyze fraudulent activities and security breaches.
   * **Helpfulness:** It plays a vital role in safeguarding financial transactions, protecting sensitive customer information, and preventing potential financial losses from cyber-attacks.
3. **E-Commerce Platforms**
   * **Use:** The system evaluates online retail environments by analyzing traffic patterns for fraudulent transactions and potential security threats.
   * **Helpfulness:** It helps secure payment information, maintain customer trust, and mitigate risks that could adversely affect the business’s reputation and operational stability.
4. **Healthcare Industry**
   * **Use:** The system assesses network security within healthcare environments to protect patient data and safeguard critical healthcare systems from cyber threats.
   * **Helpfulness:** It ensures the confidentiality and integrity of sensitive health information, supports compliance with data protection regulations, and contributes to overall data security in the healthcare sector.