# Synthesis Paper: Connecting MS-CISBA Foundations to the VulnByte Network Scanning Prototype

Cesar Ortega

VulnByte: A Web-Based IP Scanning Tool for Network Insights
Capstone CIDM 6395-75
Dr. Jeffry Babb
December 1, 2024
West Texas A&M University

## Overview

The **VulnByte** project, a web-based IP scanning tool designed for network visibility and management, serves as a capstone for the MS-CISBA program. This tool simplifies the process of scanning specific IP addresses for essential device information, and the future roadmap includes advanced features such as full network scans, port scanning, and PDF reporting. This paper explores how the foundational topics covered in the MS-CISBA program converge in the development of **VulnByte**, demonstrating the feasibility of this prototype and showcasing the interconnection of software systems, business analytics, data management, and cybersecurity.

## Foundational Qualities of the Curriculum Areas

### *Software Systems (SS)*

The **Software Systems (SS)** foundation is integral to the development of the **VulnByte** prototype, as it defines how the system is structured to integrate various components such as IP scanning, data collection, and vulnerability assessment.

In this context, **Software Engineering** principles from CIDM 6330 guided the design of a scalable architecture, ensuring that the tool can handle multiple features, from basic scans to more advanced functionalities like network-wide scans and port scanning. The tool is built using **Python**, **Django**, and **Postgres**, which offer a solid foundation for web application development. These technologies, alongside Docker for containerization, enable the creation of a flexible, scalable system capable of adapting to future requirements.

### *Business Analytics (BA)*

Business Analytics (BA) is pivotal in transforming the raw data collected from IP scans into actionable insights. The **VulnByte** tool gathers and displays critical network information such as device names, IP addresses, and MAC addresses. However, to make these details useful for network management, data must be analyzed and presented in a meaningful way.
In **CIDM 5310: Business Intelligence & Decision Support Systems**, I learned advanced **data acquisition** and **integration** techniques, as well as how to analyze and visualize data using **Power BI**. These skills were applied in **VulnByte** to create actionable insights from scan data. Additionally, I worked with **cloud services** (including **Azure**) to enable data storage and visualization, enhancing the tool's reporting functionality and supporting decision-making. The **fact-based analytics** approach and **complex data models** from this course were incorporated into **VulnByte’s** ability to provide data-driven recommendations for improving network security.

### *Data Management (DM)*

**Data Management (DM)** plays a critical role in storing, organizing, and retrieving the vast amount of scan data that **VulnByte** generates. The tool relies on **PostgreSQL** as the relational database for storing scan results, network device information, and historical data.

The CIDM 6350: Data and Information Management course taught key concepts in database design, particularly in ensuring that data is structured and indexed efficiently for retrieval. By leveraging DM principles, I have designed a database that supports the storage of scan results and allows for historical tracking, which is essential for monitoring changes in network security over time.

### *Cybersecurity and Networking (CN)*

The **Cybersecurity and Networking (CN)** domain is at the core of **VulnByte's** functionality. CIDM 6340: Networking Management and Information Security provides the theoretical and practical knowledge to integrate cybersecurity tools and frameworks into the prototype.

The core functionality of **VulnByte** includes the ability to scan IP addresses for vulnerabilities, which requires using standard security protocols and tools like **Nmap** for network discovery and vulnerability assessment. The quick and full scans available in the tool help users identify issues like open ports, device misconfigurations, and other network vulnerabilities. Additionally, the tool ensures that the data gathered during scans is securely stored, addressing compliance and security concerns relevant to network audits.

As the tool evolves, future features will extend its functionality to include port scanning and the generation of **PDF reports**, which will further enhance the tool’s capability to meet current cybersecurity needs.

## Connections Between Areas

The connection between these foundational areas is clearly demonstrated in the design and functionality of **VulnByte**:

- **Software Systems and Business Analytics**: The VulnByte web interface and backend architecture integrate the software system's core functionality, while the business analytics components transform raw data into actionable insights. These insights are presented through easy-to-understand reports and visualizations, helping users identify key vulnerabilities and manage network security effectively.
- **Business Analytics and Data Management**: **Business Analytics** relies on **Data Management** principles to ensure that the data being analyzed is properly stored, structured, and queried. The relational database design and ETL processes ensure that data is optimized for analysis, enhancing the quality of the business insights generated by the tool.
- **Data Management and Cybersecurity/Networking**: **Data Management** ensures the efficient storage and retrieval of security scan results, while **Cybersecurity and Networking** principles inform the scanning process and ensure that the tool can effectively detect vulnerabilities. The secure handling of scan data and the ability to track network security improvements over time are critical to maintaining the tool's efficacy.
- **Software Systems and Cybersecurity/Networking**: The architecture of the **VulnByte** tool supports both basic and advanced scanning features, integrating cybersecurity best practices to ensure that the system is secure, scalable, and capable of addressing evolving network security needs.

## Project Portfolio and Evolution

The **VulnByte** prototype is a culmination of the concepts and skills gained throughout the MS-CISBA program, demonstrated through projects that emphasized real-world applications of data analytics, cybersecurity, and system design:

- **CIDM 5310: Business Intelligence & Decision Support Systems**
  In this course, I learned advanced **data acquisition** and **integration** techniques, as well as how to analyze and visualize data using **Power BI**. These skills were applied in **VulnByte** to create actionable insights from scan data. I also worked with **cloud services** (including **Azure**) to enable data storage and visualization, which enhances the tool's

reporting functionality and supports decision-making. The **fact-based analytics** approach and **complex data models** from this course have been incorporated into VulnByte's ability to provide data-driven recommendations for improving network security.

- **CIDM 6340: Networking Management and Information Security**
  Through hands-on experience with security auditing and vulnerability assessments, I gained the practical knowledge required to design VulnByte's core scanning functionalities. The use of tools like Nmap ensures the tool meets professional standards for network vulnerability detection.
- **CIDM 6350: Data and Information Management**
  SQL-based projects honed my ability to design and implement relational databases. These principles are applied in VulnByte to store scan results and maintain historical records, enabling efficient data retrieval and analysis.
- **CIDM 6330: Software Engineering and Systems Development**
  In this course, I learned the principles of **software architecture** and **scalable system design**, which directly influenced the **VulnByte** project's backend architecture. The project is built using **Python**, **Django**, and **PostgreSQL**, ensuring that the system is both scalable and secure.

## Conclusion

The **VulnByte** project effectively integrates the foundational knowledge from the MS-CISBA curriculum, showcasing a cohesive application of **Software Systems**, **Business Analytics**, **Data Management**, and **Cybersecurity and Networking** principles. The prototype demonstrates the feasibility of using these areas in tandem to create a functional and scalable tool for network vulnerability scanning and management. By connecting these areas, the project not only addresses real-world security concerns but also reflects the comprehensive skill set developed throughout the program.