VulnByte: A Synthesis of Network Security and Analytics

MS-CISBA Capstone Project

Cesar Ortega

December 1, 2024

Introduction to VulnByte

- Brief overview of the project:
- A web-based IP scanning tool for network visibility and management.
- Reflects the synthesis of foundational topics (SS, BA, DM, CN).
- Future-ready with features like network scans, port scanning, and reporting.

Why VulnByte?

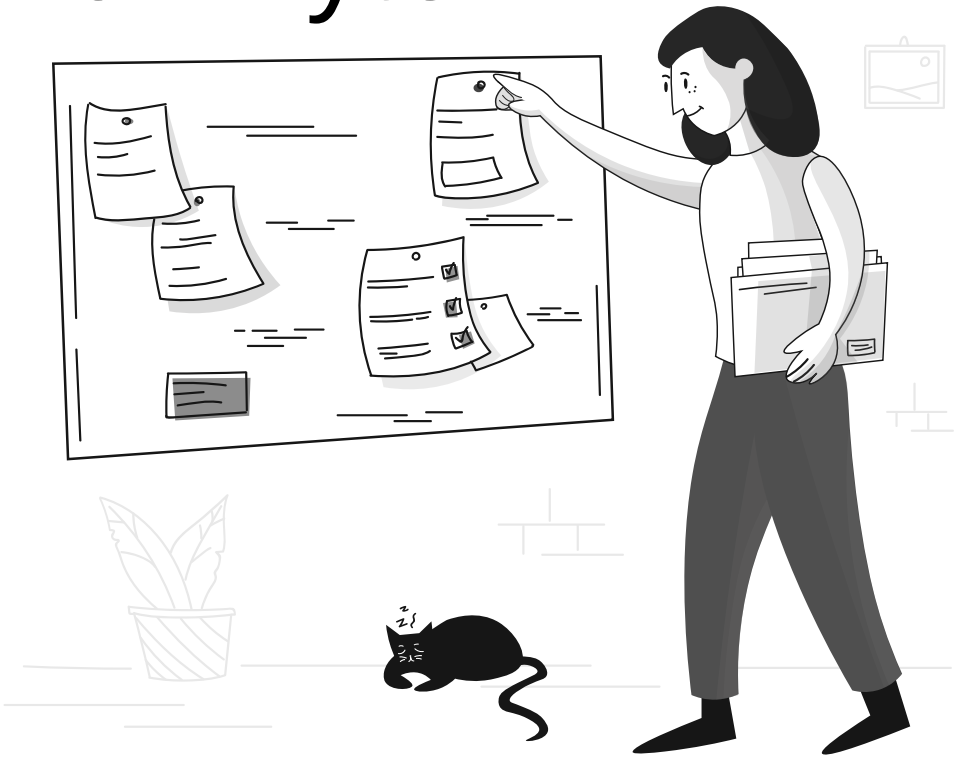
The challenges it addresses:

- Lack of accessible tools for network analysis.
- Difficulty in identifying vulnerabilities and network inefficiencies.
- Need for actionable insights for small businesses and IT professionals.

Goals of VulnByte

Key objectives:

- Simplify network security for users of varying expertise.
- Provide efficient IP scanning and vulnerability assessment.
- Deliver actionable insights through structured data and visual reports.



Illustrations by Pixeltrue on icons8

VulnByte: The Prototype

- Quick and full IP scans.
- Displays key information: IP, MAC address, device names, vulnerabilities.
- Secure database storage for scan results.

Integration of Foundational Areas

Breakdown of how VulnByte integrates:

- SS: Scalable architecture using Python, Django, and Docker.
- BA: Visual reports and insights generated from scan data.
- DM: PostgreSQL database for secure and efficient data storage.
- CN: Vulnerability detection with tools like Nmap, addressing compliance.

Synthesis Across Dimensions

Data Flow and Integration

- CN (Scanning): Performs network scans to identify IP addresses, vulnerabilities, and device details.
- Example: Using Nmap for raw data collection.
- ↓ (Data flows to storage)

- DM (Storage): Organizes and securely stores scan data in PostgreSQL for retrieval.
- Example: Historical tracking of scan results.
- ↓ (Data is analyzed)

- BA (Analysis): Converts raw data into actionable insights through visualization and predictive modeling.
- Example: Visual reports highlighting vulnerabilities and trends.
- ↓ (Insights delivered to the user)

- SS (UI & Backend): Displays insights and enables user-friendly access to data via a web-based platform.
- Example: Django-powered interface for initiating scans and viewing results.
- Integration Examples

- CN + SS: Securely transferring scan data using encryption.
- DM + BA: Structured storage optimizes reporting and analysis.
- SS + BA: Scalable interface delivers actionable insights.

VulnByte’s Future Potential

Envisioned features:

- Full network scans for comprehensive visibility.
- Port scanning for identifying open and vulnerable ports.
- PDF reporting for professional-grade summaries.
- Scalability to handle larger networks and integration with advanced analytics tools.

Future Impact of VulnByte

Benefits to users:

- Improved network security management.
- Actionable insights for proactive measures.
- Accessible tool bridging technical expertise gaps.
- Potential use cases: Small businesses, IT teams, educational institutions.

Conclusion

- Demonstrates the synthesis of MS-CISBA foundational areas.
- Reflects a cohesive and practical application of theoretical knowledge.
- Ready to evolve into a comprehensive network security solution.