Systems Analysis & Design Document

Security Configuration Management

David Lee

Dr. Walsh

4.29.2023

Table of Contents

[Project Concept 3](#_Toc133773512)

[Problem Statement 3](#_Toc133773513)

[Technology Solution 3](#_Toc133773514)

[Project Benefits 3](#_Toc133773515)

[Stakeholders 4](#_Toc133773516)

[Development Process 4](#_Toc133773517)

[Technology Tools 5](#_Toc133773518)

[Current Solutions 5](#_Toc133773519)

[Functions, Requirements, Process Map Table 6](#_Toc133773520)

[User Interface 10](#_Toc133773521)

[Wireframe 1: Dashboard 10](#_Toc133773522)

[Wireframe 2: Hosts Page 11](#_Toc133773523)

[Wireframe 3: Machine Page 12](#_Toc133773524)

[Infrastructure Architecture 13](#_Toc133773525)

[Network Topology 13](#_Toc133773526)

[Information Architecture 14](#_Toc133773527)

[Entity Relationship Diagram 14](#_Toc133773528)

[Security and Privacy Architecture 15](#_Toc133773529)

[Programming 16](#_Toc133773530)

[References 17](#_Toc133773531)

# Project Concept

This project will monitor security configurations to meet a security baseline. These will be completed via scans and the results will be stored in the form of reports. These reports can be accessed from a website.

# 

# Problem Statement

Organizations need an automated tool that can ensure Windows workstations are compliant with security standards.

# Technology Solution

Security configuration management tool for a small business to ensure security compliance.

# Project Benefits

* Will ensure security compliance with federal and state regulations.
* Will save resources both in time and money.
* Shows the organization’s good faith in protecting client data.

# Stakeholders

Stakeholders of this project will benefit directly are the Legal and IT departments along with public relations. Legal will benefit from this project in a legal sense according to the PESTEL framework. It will ensure the organization is compliant with federal and state regulations. In doing so, the risk of legal action is mitigated.

Next is the IT department. This project benefits the IT department since it will save time and money as it will automate tasks. This will save resources that can benefit the entire organization. In the context of PESTEL, this is a technological factor.

The last stakeholder mentioned here is public relations. Again, according to PESTEL it will benefit as a social factor since the public is becoming more concerned about how safe their data is (Maurer, 2021). By taking steps to secure our systems, If an incident where to go public, the organization could show due diligence and reduce public backlash in the long term.

# Development Process

For the planning, analysis, and design phase, the Waterfall method will be used. The benefit of the waterfall method is its rigid dependent approach to completing tasks. This is ideal for the early steps of the SDFC as it lays a solid foundation for the implementation and support phases of the project.

As hinted above, the implementation and support phases will not use the waterfall method. Instead, those phases will use the agile methodology. Agile is ideal for later phase as it will be able to adapt to changes in requirements and any unforeseen challenges.

# Technology Tools

This project will be full-stack. Meaning it will have a front-end, middle-ware, and a back-end. Starting with the front-end. It will be done with Bootstrap and flask. Bootstrap is a popular CSS framework for developing websites. Flaks is a popular python web framework that will connect to the database.

Next is the middleware. The middleware will be written in PowerShell and will run on windows desktops. These PowerShell scripts will collect the configuration of the host system and compare it to a security baseline. The results of the comparison will be packaged in JSON and forward to the MongoDB; both of which are JSON friendly.

The database that this project will utilize MongoDB. This database is ideal as it works well with storing JSON files. In fact there is a version of MongoDB made specifically for JSON files. All of the tools mentioned here have documentation of how to integrate.

# Current Solutions

There are many configuration management tools available. To name a few there are Chef, Puppet, Saltstack, and Ansible (Simplilearn, 2018). All check system configurations and compare them to a baseline. However, none of these solutions create automatic reports or offer redundancy. This is where this project brings value. Chef and Puppet are stateful configuration managers that rely on applications on the host machine to conduct tasks. Ansible on the other hand is stateless and will login to the machine to conduct tasks. This has less overhead on each host, however if the ansible server where to fail, reports will never be generated. This does not offer redundancy. By having the tasks indicated locally and forwarded to a backup server, redundancy is assured.

## Functions, Requirements, Process Map Table

|  |  |
| --- | --- |
| **FUNCTION** | **REQUIREMENTS** |
| **Scan local host to measure security compliance**  This PowerShell script will compare the current security configuration to the target security configuration. It will write the results of the scan to a JSON file along with metadata for future reference. Powershell’s built in feature to export objects as a JSON files is key to this function. | * A PowerShell script will run on a windows machines * Schedule scan to run weekly * Collect current security configuration state * Pull target security configuration state * Compare current and target states * Store comparison results locally as a JSON * Add following fields to report * Scan date * Host name * IP address * Firewall * Firewall service * UAC * Windows update service * Windows defender status * SMB1 disabled * All tests will be Pass/Fail grade |
|  | |
| **Forward and store compliance scan reports in a database**  The built-in PowerShell feature to forward files to a MongoDB database. There the reports will be stored as JSON files until retrieval. | * Forward to MongoDB database for storage * Database needs to be able to accept JSON files forwarded by PowerShell over the intranet |
| Diagram  Description automatically generated | |
| **Retrieve Reports**  The user will request to download a report by clicking the corresponding link. The bootstrap-built webpages will use flask APIs to query the MongoDB database for reports as JSON files. | * Retrieve reports with flask * Data stored in database need to be retrievable by the flask web framework * Database API need to be compatible with flask API |
|  | |
| **Present reports**  There will be various way to view the organizations security compliance. They boil down to managerial views with the ‘Dashboard’ page and more detailed views with the ‘Hosts’ and ‘Machine’ pages. The reports will be converted to PDF for readability. By converting the report from JSON to PDF, the report can easily be emailed or forwarded to appropriate staff to make any non-machines compliant. | * Monitor for non-compliant machines * Create a notification if a machine is non-compliant * A page will list number of compliant and non-compliant hosts * Page will list compliant and non-compliant hosts * A page will list all hosts their compliant status * A page will list each machine’s report history * Reports can be downloaded as a PDF |
|  | |

# User Interface

## Wireframe 1: Dashboard

This page lists the last scheduled scan time and date. The number of compliant and noncompliant hosts it also lists the host names below. This provides a high-level view of the organization’s security compliancy. In doing so, managers and technicians alike will have more visibility into the network.

Table

Description automatically generated

## Wireframe 2: Hosts Page

Displays hostname, status, and linked reports. This page is made to view all hosts. like the ‘Dashboard’ but also shows them in with the actual scan date and provides a link to the report. This page is more for technicians than management.

Table

Description automatically generated

## Wireframe 3: Machine Page

Display hostname, status, date, and links to their previous reports. This page has all the reports associated with a host. This is accessed by clicking on the host name of a machine on the ‘Dashboard’ or ‘Hosts’ pages. This allows technicians to see the compliance history of a machine.

Table

Description automatically generated

# Infrastructure Architecture

## Network Topology

Diagram

Description automatically generated

# Information Architecture

## Entity Relationship Diagram

Note this is a non-SQL database ERD. Therefore, it is a logical representation of has the data is used per Dr. Walsh’s request.

Diagram

Description automatically generated

# Security and Privacy Architecture

System security configuration is sensitive information. It is essentially a report of a system’s strengths and potential weaknesses. If an adversary is able to access this data, they will have knowledge of a system without having to risk exposing themselves via scans on the network. This is why Access management is put in place on each system to prevent unauthorized access to reports. On the other hand, logs from a critical phase of an incident could be equally disastrous. As such, there need to be redundancies in report storing. Data will be stored locally on the machine and in the MongoDB. All of these have access management in place to prevent these scenarios.

# Programming

Powershell - Performs business process. It is native to windows systems and thus allows for easy integration with the preexisting environment. This would mean no additional licensing costs when implementing the business logic.

MongoDB document database - NoSQL database that doesn’t use relationships to structure it’s data. MongoDB has a version that is made specifically for JSON files. This is ideal as the data will always be in JSON format when in transit. In addition, PowerShell has a feature that allows forwarding files to MongoDB databases.

JSON - versatile format for storing and transmitting data. compatible with all tools listed here. It is also the industry standard for logging. Meaning if the organization does outgrow this solution, It can more easily integrate these reports into future solutions.

Flask - web framework that will provide the API that allows the front-end to query the database. It is compatible with Bootstrap and MongoDB APIs.

Bootstrap - HTML and CSS front-end. It is compatible with flask. This will contribute to a clean user-friendly front end.

# References

Maurer, T. (2021, March 16). *We must defend against the cyber threats facing our global financial systems*. CNN. https://edition.cnn.com/2021/03/14/perspectives/global-cyber-threat-imf-perspectives

S. (2018, September 25). *What Is Ansible? | How Ansible Works? | Ansible Playbook Tutorial For Beginners | DevOps|Simplilearn* [Video]. YouTube. https://www.youtube.com/watch?v=wgQ3rHFTM4E&feature=youtu.be

Dyouri, Abdelhadi. “How to Use MongoDB in a Flask Application.” *DigitalOcean*, DigitalOcean, 14 Feb. 2022, https://www.digitalocean.com/community/tutorials/how-to-use-MongoDB-in-a-flask-application.

“Flask Server: How Does Flask Server Work with Examples?” *EDUCBA*, 19 Apr. 2023, https://www.educba.com/flask-server/.

“What Is JSON?” *What Is JSON*, https://www.w3schools.com/whatis/whatis\_json.asp.

Editor. “How to Use Bootstrap with Flask.” *Blog*, Blog, 3 Oct. 2021, https://blog.appseed.us/how-to-use-bootstrap-with-flask/.

“Flask-Pymongo with MongoDB Atlas Guide.” *MongoDB*, https://www.MongoDB.com/compatibility/setting-up-flask-with-MongoDB.

“What Is Nosql? NoSQL Databases Explained.” *MongoDB*, https://www.MongoDB.com/nosql-explained.