Lab #3 – Docker Image Security: Static Analysis Tool

Overview

This lab will build from the previous Docker lab and follow best practices in Docker Security by scanning docker images for vulnerabilities using a static analysis tool called Trivy.

Preparation

Have a working containerized application with a built Docker image that runs as a container successfully.

Image Vulnerability Scanning

For this part, we will implement a static analysis tool for Docker images called Trivy. Trivy performs image vulnerability scanning by identifying the packages & versions in images and then cross-referencing them with vulnerability databases.

1. Download and install Trivy
   `https://github.com/aquasecurity/trivy`

2. Update image to use a vulnerable base image in the Dockerfile as follows:
   ```
   FROM node:lts-alpine3.9
   ```

   Rebuild and Run your Docker image – the process should complete successfully.

3. Scan for vulnerabilities using trivy

Screenshots

Show a screenshot or screenshots that are identifiable with your account name/environment showing this is working and implemented as specified.

Reflection

1. Record any of your own observations, solutions, or comments about the work you did. What problems did you have, what was not clear, what did you take away that you value? If everything went great, what did you see while you were doing it that you are looking to investigate more – or did investigate? Explain and make clear your configuration choices. This is mandatory.

2. In your own words, with any websites you gain information from listed as references, and without just using a thesaurus to change words that are copy and pasted from such a website, tell us about how one could implement image vulnerability scanning as a part of their development processes? (note: the best way to avoid academic issues with writing this sort of thing is ready on the topic, put that web page away, and write it from your knowledge; if you have difficulty, just read it, talk about it with your professor or a friend, and then write again in your own understanding).