Image Hardening

Hadolint: A linter for Dockerfiles that helps to find and fix common issues and security vulnerabilities

How to install Hadolint

Step 1: Download the latest Linux Hadolint package from Hadolint Github Release page.

wget -O hadolint https://github.com/hadolint/hadolint/releases/download/v2.12.0/hadolint-Linux-x86_64

Step 2: Once you downloaded the application, move it to the /usr/local/bin directory.

sudo mv hadolint /usr/local/bin/hadolint

Step 3: Give execution permission to Hadolint using the command given below.sudo

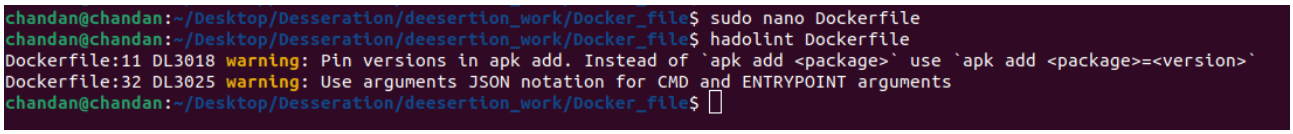
chmod +x /usr/local/bin/hadolint

Step 4: To check if Hadolint is installed on your Linux or Mac system, run the command:
hadolint --version

How to check docker issues with hadolint

Just need to use hadlonit packge to scan docker file

And it gives all the issues to address based on our image. It suggests adding APK packages and their versions, and also recommends using CMD and ENTRYPOINT.



Docker file we used to Image Hardening

Use an official Nginx image with Alpine Linux from Docker Hub

FROM nginx:alpine

Set maintainer label

LABEL maintainer="chandanshankar1999@gmail.com"

Remove default server definition

RUN rm /etc/nginx/conf.d/default.conf

Install fail2ban

```
RUN apk update && \
    apk add --no-cache fail2ban && \
    mkdir -p /etc/fail2ban/filter.d

# Copy your Nginx configuration file
COPY nginx.conf /etc/nginx/nginx.conf

# Copy fail2ban configuration
COPY fail2ban/jail.local /etc/fail2ban/jail.local
COPY fail2ban/filter.d/nginx-http-auth.conf /etc/fail2ban/filter.d/nginx-http-auth.conf

# Copy custom Python script
COPY scripts/monitor_logs.py /usr/local/bin/monitor_logs.py

# Set file permissions
RUN chmod -R 644 /etc/nginx/nginx.conf

# Expose ports
EXPOSE 80 443

# Start Nginx and fail2ban
CMD service fail2ban start && nginx -g 'daemon off;'
```