

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 8

**Scenario :** You are a DevOps engineer working for a software development company that is transitioning its applications to containerized environments using Docker. As part of the migration process, you are responsible for ensuring the security and reliability of containers and container images. Your team has developed a web application that is ready for deployment in a containerized environment.

Your task is to assess the security and integrity of the container and image for the web application before it is deployed to production. Your assessment should cover potential vulnerabilities, security best practices, and ensure that the containerized application is properly configured and functional.

Steps and Screenshots :



Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 8

A screenshot of a Linux desktop environment, likely elementary OS, showing a terminal window. The terminal window has a light gray background and a dark blue header bar. The header bar displays system status icons (battery at 30%, signal strength, volume), the date and time (08:23 AM), and the current working directory (~/Documents). The terminal itself shows a command-line session where the user runs 'hadolint NodeApp/Dockerfile'. The output of the command includes several warning messages from 'hadolint' about Dockerfile syntax and pinning npm package versions. The desktop interface below the terminal includes a dock with various application icons (e.g., Dash, Home, File Manager, Terminal, Browser, Mail, etc.) and a taskbar with open application windows.

```
yl .../ 08:23 hadolint NodeApp/Dockerfile
NodeApp/Dockerfile:8 DL3016 warning: Pin versions in npm. Instead of `npm install <package>` use `npm install <package>@<version>`.
NodeApp/Dockerfile:8 DL3059 info: Multiple consecutive 'RUN' instructions. Consider consolidation.

yl .../ 08:23 |
```

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 8

## 2. Change dockerfile contents and optimize it and scan again till no suggestions are left

The screenshot shows a code editor interface with a Dockerfile open in the main pane. The Dockerfile content is as follows:

```
FROM node:12.11.1-alpine
WORKDIR /usr/src/app
COPY package*.json .
# Install app dependencies
# A wildcard is used to ensure both package.json AND package-lock.json are copied
COPY server.js .
RUN npm install
RUN npm install express@4.21.0
COPY .
EXPOSE 8080
CMD [ "node", "server.js" ]
```

In the terminal pane below, the command `hadolint ./Dockerfile` is run, resulting in the following output:

```
./Dockerfile:8 DL3059 info: Multiple consecutive 'RUN' instructions. Consider consolidation.
```

A status bar at the bottom indicates "Command failed: java -DRHDA\_TOKEN=92fdf101-55e5-45bf-9330-c07a..."

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 8

The screenshot shows a terminal window within a code editor interface. The terminal output is as follows:

```
no suggestions now, everything fixed

ydl _/NodeApp 1^ main ? @ v22.9.0 11:42 hadolint ./Dockerfile
./Dockerfile:8 DL3016 warning: Pin versions in npm. Instead of `npm install <package>` use `npm install <package>@<version>`' ./Dockerfile:8 DL3059 info: Multiple consecutive 'RUN' instructions. Consider consolidation.

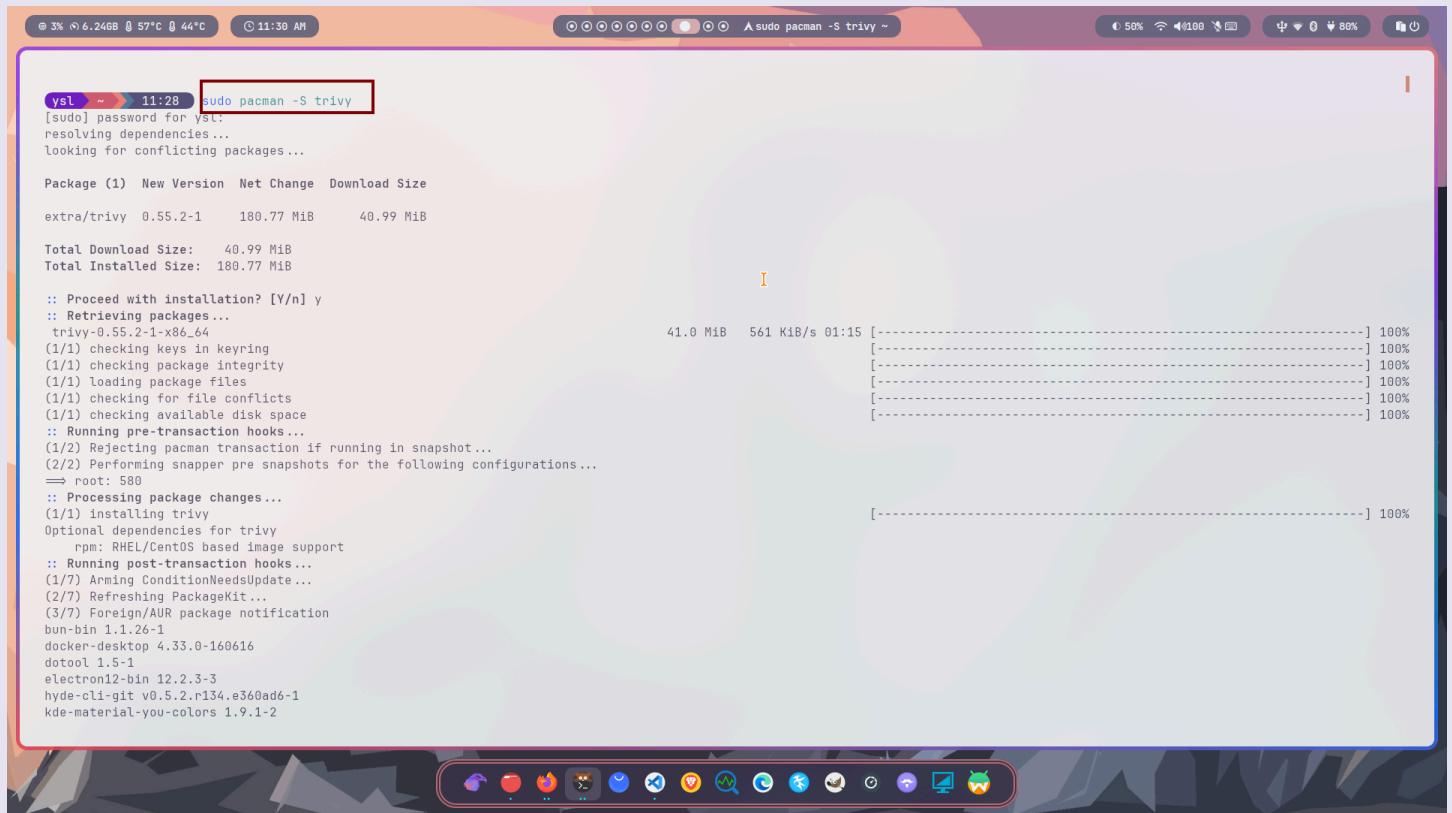
ydl _/NodeApp 1^ main ? @ v22.9.0 11:42 hadolint ./Dockerfile
./Dockerfile:8 DL3059 info: Multiple consecutive 'RUN' instructions. Consider consolidation.

ydl _/NodeApp 1^ main !? @ v22.9.0 11:48 hadolint ./Dockerfile
ydl _/NodeApp 1^ main !? @ v22.9.0 11:49 hadolint ./Dockerfile
```

A red box highlights the command `hadolint ./Dockerfile` in the final line of the terminal output.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 8

### 3. Install trivy and scan the docker image built using it



```
yal ~ 11:28 sudo pacman -S trivy
[sudo] password for yst:
resolving dependencies...
looking for conflicting packages...

Package (1) New Version Net Change Download Size
extra/trivy 0.55.2-1 180.77 MiB 40.99 MiB

Total Download Size: 40.99 MiB
Total Installed Size: 180.77 MiB

:: Proceed with installation? [Y/n] y
:: Retrieving packages...
trivy-0.55.2-1-x86_64
(1/1) checking keys in keyring
(1/1) checking package integrity
(1/1) loading package files
(1/1) checking for file conflicts
(1/1) checking available disk space
:: Running pre-transaction hooks...
(1/2) Rejecting pacman transaction if running in snapshot...
(2/2) Performing snapper pre snapshots for the following configurations...
== root: 580
:: Processing package changes...
(1/1) installing trivy
Optional dependencies for trivy
    rpm: RHEL/CentOS based image support
:: Running post-transaction hooks...
(1/7) Arming ConditionNeedsUpdate...
(2/7) Refreshing PackageKit...
(3/7) Foreign/AUR package notification
bun-bin 1.1.26-1
dockerd-desktop 4.33.0-160616
dotool 1.5-1
electron12-bin 12.2.3-3
hyde-cli-git v0.5.2.r134.e360ad6-1
kde-material-you-colors 1.9.1-2

41.0 MiB 561 KiB/s 01:15 [-----] 100%
[-----] 100%
[-----] 100%
[-----] 100%
[-----] 100%
[-----] 100%
```

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 8

A screenshot of a Linux desktop environment. The terminal window shows the command `docker build -t prac8-yasl .` being run, which successfully builds a Docker image named `prac8-yasl`. The Dockerfile in the project root contains the following code:

```
FROM node:12.11.1-alpine
WORKDIR /usr/src/app
COPY package-lock.json .
RUN npm install express@4.21.0
COPY .
EXPOSE 8080
CMD ["node", "server.js"]
```

The terminal also shows the command `trivy image prac8-yasl` being run, but it fails with fatal errors related to Docker daemon connectivity and Podman socket issues.

A screenshot of a Linux desktop environment. The terminal window shows the command `trivy image prac8-yasl` being run, which completes successfully with no vulnerabilities found. The Dockerfile and build logs are identical to the previous screenshot.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 8

The screenshot shows a terminal window with the following output:

```
ysl ~/NodeApp 12 main !? @ v22.9.0 12:31 trivy image prac8-ysl
2024-09-30T12:31:50+05:30 INFO [vuln] Vulnerability scanning is enabled
2024-09-30T12:31:50+05:30 INFO [secret] Secret scanning is enabled
2024-09-30T12:31:50+05:30 INFO [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-09-30T12:31:50+05:30 INFO [secret] Please see also https://aquasecurity.github.io/trivy/v0.55/docs/scanner/secret#recommendation for faster secret detection
2024-09-30T12:31:50+05:30 INFO Detected OS family="alpine" version="3.9.4"
2024-09-30T12:31:50+05:30 INFO [alpine] Detecting vulnerabilities... os_version="3.9" repository="3.9" pkg_num=16
2024-09-30T12:31:50+05:30 INFO Number of language-specific files num=1
2024-09-30T12:31:50+05:30 INFO [node-pkg] Detecting vulnerabilities...
2024-09-30T12:31:50+05:30 WARN This OS version is no longer supported by the distribution family="alpine" version="3.9.4"
2024-09-30T12:31:50+05:30 WARN The vulnerability detection may be insufficient because security updates are not provided

prac8-ysl (alpine 3.9.4)

Total: 24 (UNKNOWN: 0, LOW: 4, MEDIUM: 14, HIGH: 6, CRITICAL: 0)
```

A red annotation box highlights the following text in the terminal output:

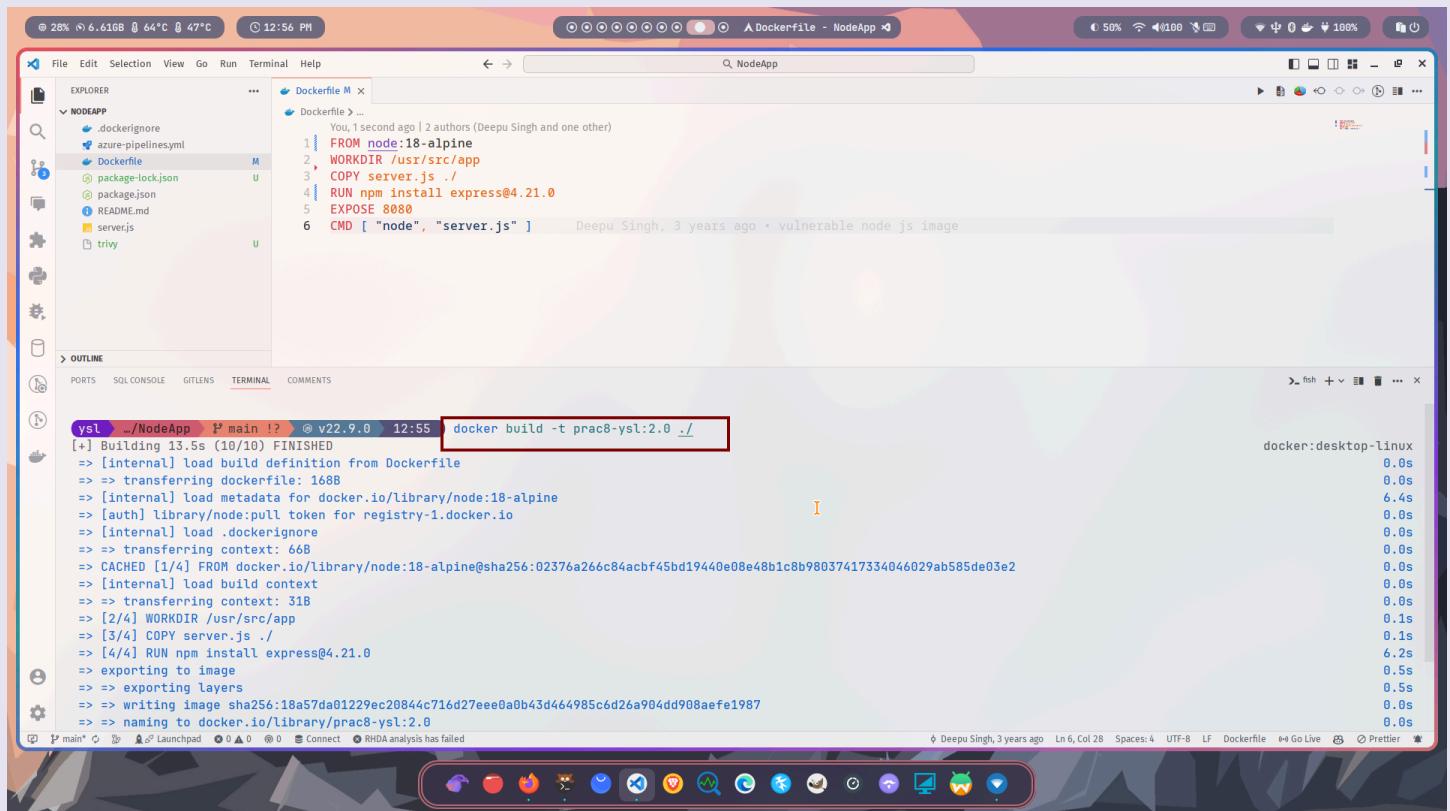
now docker socket is found by trivy in /var/run/ folder  
as we have created its soft link from our local machine's  
docker socket to the folder in which trivy is scanning it

Below the terminal, there is a table showing the results of the vulnerability scan:

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
libcrypto1.1	CVE-2020-1967	HIGH	fixed	1.1.1b-r1	1.1.1g-r0	openssl: Segmentation fault in SSL_check_chain causes denial of service

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 8

#### 4. Now fix dockerfile and optimize it (upgrade base os and packages and optimize copy, run commands)



The screenshot shows a terminal window with the following command and its output:

```
ysl ~/NodeApp $ main !? @ v22.9.0 12:55 docker build -t prac8-ysl:2.0 .
```

[+] Building 13.5s (10/10) FINISHED  
=> [internal] load build definition from Dockerfile  
=> => transferring dockerfile: 168B  
=> [internal] load metadata for docker.io/library/node:18-alpine  
=> [auth] library/node:pull token for registry-1.docker.io  
=> [internal] load .dockignore  
=> => transferring context: 66B  
=> CACHED [1/4] FROM docker.io/library/node:18-alpine@sha256:02376a266c84acbf45bd19440e08e48b1c8b98037417334046029ab585de03e2  
=> [internal] load build context  
=> => transferring context: 31B  
=> [2/4] WORKDIR /usr/src/app  
=> [3/4] COPY server.js ./  
=> [4/4] RUN npm install express@4.21.0  
=> exporting to image  
=> => exporting layers  
=> => writing image sha256:18a57da01229ec20844c716d27eee0a0b43d464985c6d26a904dd908aefef1987  
=> => naming to docker.io/library/prac8-ysl:2.0

The terminal also displays system status at the top and a docked application bar at the bottom.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 8

## 5. Now scan and see there should be no vulnerabilities in image

The screenshot shows a terminal window with the following command and its output:

```
ysl .../NodeApp $ main !? @ v22.9.0 12:56 trivy image prac8-ysl:2.0
```

Output:

```
2024-09-30T12:56:21+05:30 INFO [vuln] Vulnerability scanning is enabled
2024-09-30T12:56:21+05:30 INFO [secret] Secret scanning is enabled
2024-09-30T12:56:21+05:30 INFO [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-09-30T12:56:21+05:30 INFO [secret] Please see also https://aquasecurity.github.io/trivy/v0.55/docs/scanner/secret#recommendation for faster secret detection
2024-09-30T12:56:28+05:30 INFO Detected OS family="alpine" version="3.20.3"
2024-09-30T12:56:28+05:30 INFO [alpine] Detecting vulnerabilities... os_version="3.20" repository="3.20" pkg_num=16
2024-09-30T12:56:28+05:30 INFO Number of language-specific files num=1
2024-09-30T12:56:28+05:30 INFO [node-pkg] Detecting vulnerabilities...
```

prac8-ysl:2.0 (alpine 3.20.3)

Total: 0 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 0)

At the bottom, it says "RHDA analysis has failed".