# Static analysis for dockerfile

Vilho Aaltonen
COMP.SEC.300
10.5.2023

# Docker

- Docker allows developer to create and run software in portable environments called containers
- Docker is widely used
  - In february 2022 there were over 15 million users (source)
- Docker container is based on *Docker image*
- Simple way to create Docker *image* is to define it in a *Dockerfile*

# Dockerfile

- Dockerfile is a text file where Docker image is defined
- The format for file is: **INSTRUCTION arg1, arg2…**
- Only mandatory instruction is **FROM** that tells the *base image* and starts a new build stage

# Dockerfile example content

```
FROM node:18-alpine
WORKDIR /src
COPY . /src/
RUN npm install
CMD ["node", "./index.js"]
EXPOSE 4200
```

# Why analysis

- When writing Dockerfile there are few risks that may cause security issues
- Checking file before building image from it could reduce this risk significantly
- Few examples
  - Container would be executed with root privileges
  - Base image itself is not secure
  - Exposing ports that are reserved for OS

# Technologies

- Python 3.9
- File is parsed with dockerfile_parse
- Unit test implemented with pytest
- Requires that there is a Docker client at machine
  - This is used to check base image trust status

# Demo Dockerfile

```
# Nonsense to get errors
FROM myUntrustedBaseImage
WORKDIR /app
ADD . .
RUN yarn install --production
CMD ["node", "src/index.js"]
EXPOSE 10
```

# Demo output

Add specific tag to the base image

Prefer COPY over ADD at line 5

No USER tag found. This may mean that container is executed with root privileges.

Avoid well-known ports, use ports higher than 1024 current value 10 at line 8

mySuspiciousBaseImage

Couldn't verify that image is trusted

# Things to improve

- Found more vulnerabilities
- Add colours to output to make it more readable
- Refactor the code