Task 3.C: Securing Docker

1- What runtime security scanner you used

I used Falco 0.39.1, a runtime security tool designed to monitor and detect irregular behaviour in containers and Linux systems, running inside a Docker container.

2- 2. The image used, or the Dockerfile to build it

I pulled the official Falco Docker image:

Image Used: falcosecurity/falco-no-driver:latest

```
sudo docker pull falcosecurity/falco-no-driver:latest
```

3- Screeshots attached

4- 4. What commands and/or activities used to trigger the alerts

I triggered security alerts by starting a privileged container. The use of the --privileged flag is considered a suspicious action by Falco.

```
sudo docker pull ubuntu
sudo docker run --rm -it --privileged ubuntu bash
```

Commands Used:

- Pull the Falco Image:
  bash
  ```
  sudo docker pull falcosecurity/falco-no-driver:latest
  ```
- Run Falco:
  bash
  ```
  sudo docker run --rm -it --privileged -v
  /var/run/docker.sock:/host/var/run/docker.sock -v /proc:/host/proc:ro -v
  /etc:/host/etc:ro falcosecurity/falco-no-driver:latest
  ```
- Trigger an Alert by Running a Privileged Ubuntu Container:
  bash
  ```
  sudo docker run --rm -it --privileged ubuntu bash
  ```