* As security practices please follow below steps while executing the assignment and evaluation
* While creating Docker file use Copy instead of ADD
* Avoid running containers as root
* Never put secrets or credentials in Docker file instructions use .docker ignore
* In Docker file add metadata and labels.
* Leverage linters to automatize checks.

1. Create a docker bridge docker network with name hu-devops-sdet1.0.
2. Create a Dockerfile to create a web server nginx container with customized html page, and run on port number 99 not with the default port and run it on the previously created network.
3. Locally scan the Docker file using linter and fix if any warning are there.
4. Once your containers are up and running, store your container logs in a file and mount that file at your localhost.
5. Push your Docker image into the DockerHub private repository with appropriate tagging "YourName-HU-SDET 1.0-versionnumber",push the image with multiple versions.
6. Write a Docker-compose file for a web server Apache and expose with a port number 2000.
7. Document the complete process with Screenshots.