**Docker Vulnerability Scan**

In this exercise, we will run Vulnerability scan on a docker image.

1. Create an Ubuntu instance with t2.micro.
2. Connect to the instance using putty.
3. Run the following commands for installing docker and pull golang image for testing.

sudo apt update && sudo apt install docker.io -y

sudo docker pull golang

1. Test the application.
   1. Install the Vulnerability Scan tool.

sudo apt-get install wget apt-transport-https gnupg lsb-release

wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | gpg --dearmor | sudo tee /usr/share/keyrings/trivy.gpg > /dev/null

echo "deb [signed-by=/usr/share/keyrings/trivy.gpg] https://aquasecurity.github.io/trivy-repo/deb $(lsb\_release -sc) main" | sudo tee -a /etc/apt/sources.list.d/trivy.list

sudo apt-get update

sudo apt-get install trivy

* 1. Run the test command. Analyse the report.

sudo trivy image golang

1. Terminate the instance.