

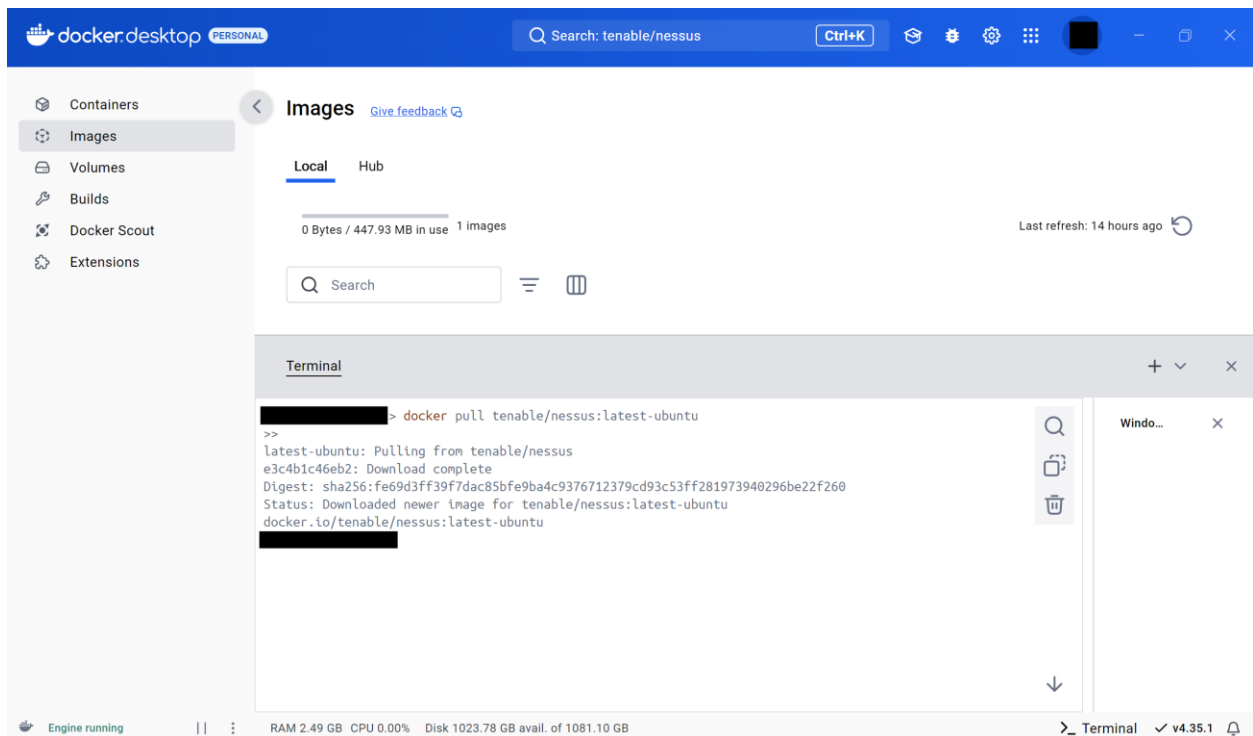
Running Nessus in Docker

Project:

In this project, I set up an instance of Nessus in Docker and then conducted host discovery and vulnerability scans on a LAN.

Pull the Nessus Docker Image:

I pulled the Nessus Docker image from Docker Hub, specifying the latest Ubuntu version.

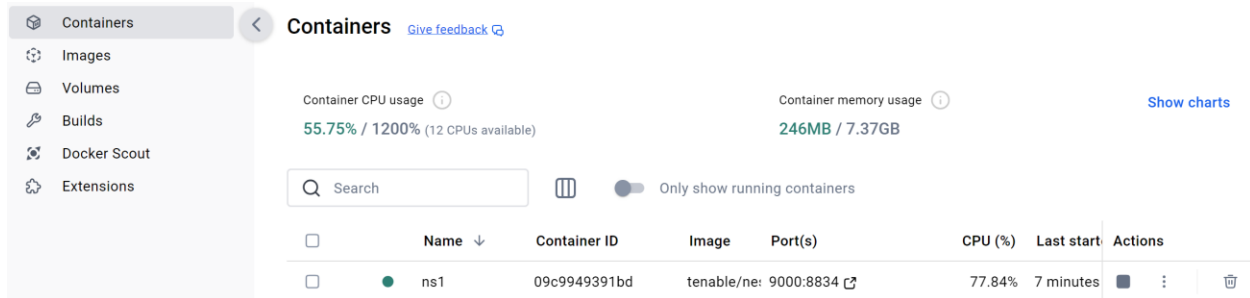


Create and Run the Docker Container:

I used the `--name` command to name the container “ns1”, the `-p` command to map the container port 8834 to my machine’s port 9000, and the `-d` command to run the container in detached mode.

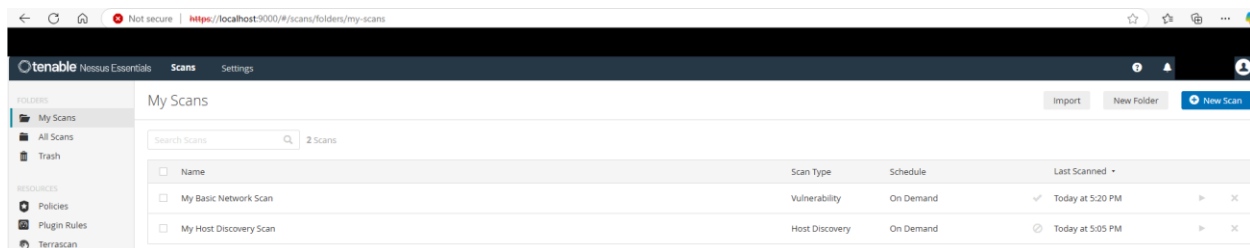
```
docker run --name ns1 -p 9000:8834 -d tenable/nessus:latest-ubuntu
```

Container with Live Nessus Instance:



Connecting to the Nessus Web Interface and Performing Scans:

I accessed the Nessus web interface by opening a web browser and navigating to <https://localhost:9000>. I then ran a host discovery and network vulnerability scan to ensure the software was functioning properly, which it was.



Conclusion:

In this project I pulled a Nessus Docker image from Docker Hub, I then created a container using said image and ran the container. I then accessed the Nessus web interface by opening a web browser and navigating to <https://localhost:9000> and ran a couple of basic scans to make sure the instance was functioning properly.