MID-TERM PROJECT REVIEW REPORT

Team Members

Poonam Kashyap (M21CS012)
Abhijit S Iyer (M21CS001)

Project Title

An analysis of *Docker* from a security perspective, based on the research paper To Docker or Not to Docker: A Security Perspective

Problem Statement

Existing security implementations on docker containers focus mainly on the relationship between the host machine and the container. However, today, Docker containers are now part of a complex ecosystem, which includes containers and various repositories and orchestrators, that is highly automated. Container solutions embed automated deployment chains that are meant to speed up the code deployment processes. These chains are often composed of third-party elements running on different platforms provided by various providers, raising concerns about code integrity. This can cause multiple vulnerabilities that an adversary could exploit to penetrate the system. Container ecosystem security has yet to be thoroughly investigated, despite being fundamental to container adoption. The primary reasons why we focus on the Docker ecosystem are:

- Docker as a container system is already being used/ will be used by almost 92% of DevOps systems.
- Security is the first barrier to the adoption of this container environment.
- Docker is already running in some environments, making it possible to run experiments and explore the practicality of some attacks.

Current Progress

- A thorough analysis of the research paper has been done. We have prepared a summary document of the research paper for future reference, noting down the key aspects of the research paper that will help us proceed with the implementation of our project.

- We are getting used to the environment of Docker and learning how the features of docker and deployment of applications on Docker containers is being done so that we get a first-hand feel of the whole ecosystem, thereby allowing us to get acclimatized to the environment before we can start working on the project.
- We are on the lookout for references available in a research paper to understand the vulnerabilities better, trying to get a clear picture of how we are supposed to reproduce vulnerable security scenarios.

Plans to complete the remaining work

- We will start recreating scenarios that were mentioned in the research paper that lead to certain vulnerabilities which were detected in the Docker ecosystem.
- We will look to experiment with the docker environment by deploying applications and possibly find out new security flaws in the Docker container system so that those flaws can also be reported and specified along with the existing flaws.
- We will prepare a thorough report on our analysis of the research paper, our work on the reproduction of the vulnerabilities in the system, and also our contribution to finding out new vulnerabilities in the system.

Contribution of each member

Common Contributions:

Poonam and Abhijit worked on analysing and examining the research paper, trying to understand the motivation behind this project, and trying to figure out how vulnerable the Docker system is. They also worked on understanding the docker ecosystem, how applications are deployed, and the different available features of docker.

Poonam Kashyap:

Poonam worked on examining the various references that were made in the research paper, trying to understand from the core sources how vulnerabilities were found out and how they were addressed. She will also work in recreating the vulnerabilities on the docker ecosystem, exposing the security vulnerabilities.

Abhijit S Iyer:

Abhijit worked on preparing the concise summary document of the research paper that contains the key aspects of the study of the research that will help us proceed with the implementation of our project. In addition to that, Abhijit will also look to find out new flaws in the docker system by deploying applications and experimenting with the system so as to check on the stability of Docker.