Гураль К.В.

INVESTIGATION OF VULNERABILITIES IN PROCESS CONTAINERIZATION TOOLS ON THE EXAMPLE OF DOCKER

Vinnytsia National Technical University

Анотація

У статті досліджені основні вразливості системи контейнеризації Docker та їх класифікація за рівнями безпеки. Проаналізована частка потенційно вразливих Docker образів у публічному офіційному реєстрі образів Docker Hub.

Ключові слова: контейнеризація, Docker, контейнер, вразливість, Docker образ, інформаційна безпека.

Abstract

The article examines the main vulnerabilities of Docker containerization system and classifies them by security levels. The fraction of potentially vulnerable Docker images in official public registry Docker Hub is being analyzed.

Keywords: containerization, Docker, container, vulnerability, Docker image, information security.

Intro

55.06% of all respondents, answering the question “Which tools have you done extensive development work in over the past year, and which do you want to work in over the next year?”, chose Docker, according to Stack Overflow annual developer survey in 2021. In addition, 29.7% of respondents chose it as the most wanted tool to learn and it is considered the second most loved tool - his means that specialists who use it are satisfied with a technology [1].

Nowadays, being the leader of containerization market, Docker affects the whole IT industry dramatically, and using this technology, one must be aware of its vulnerabilities.

Docker Hub Images vulnerabilities

According to public report of Prevasio, a cyber security start-up, in 2020 among 4M of publicly available Docker Hub container images:

- 51% - over 2 million images - contain one or more packages or application dependencies with at least one critical vulnerability;
- 20% are considered to be non-harmful;
- 13% are considered to have high-level vulnerabilities;
- 4% contained moderate vulnerabilities;
- 6,432 were found to be malicious or potentially harmful, representing 0.16% of the entire Docker Hub registry. The total pull count of these images is over 300 million [2].

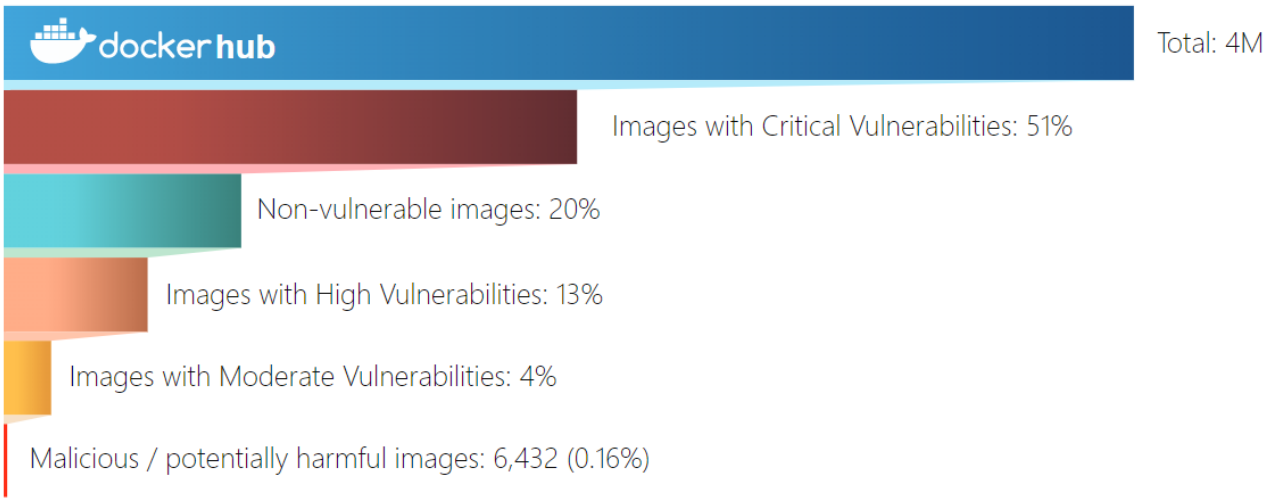

Figure 1 – Diagram of images' vulnerability distribution in Docker Hub [2]

Layers of Docker security

Conventionally, the security layers of the Docker infrastructure can be divided into two major categories. The first is everything that relates directly to the containers and the host on which the containers are running. The second is the external components of the infrastructure – there go also additional actions to increase the security of the entire container system [3].

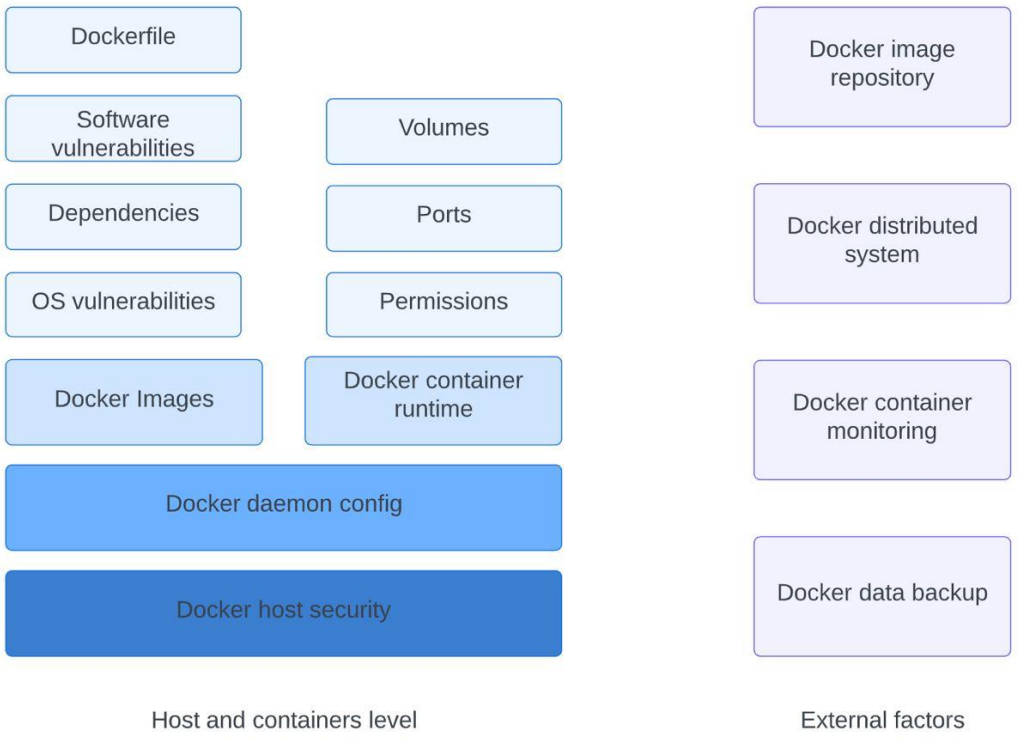

Figure 2 – Levels of Docker security

Let's dive deeper into every layer:

1. **Docker host security** - everything related to the security of the host on which the containers are running. Compromising a host will most likely compromise all containers on that host.
2. **Docker Daemon config** - specific settings and features of the Docker Daemon (also known as Docker Engine), which is serving running containers directly.

3. **Docker images** - the scope of the attacks, which are related to Docker images themselves. Problems in this layer appear mainly during the image build.
    a) OS Vulnerabilities - vulnerabilities in the base image and system packages included in this image
    b) Dependencies - vulnerabilities in a third-party dependencies that are pulled and then used in applications inside containers
    c) Software Vulnerabilities are specific vulnerabilities in the applications for which containers were created. This includes all the problems with the code of these applications itselves.
    d) Dockerfile - incorrect and unsafe instructions that can be used when assembling an image.
4. **Docker container run-time** - all the problems that are associated with the run-time configuration of containers, that is, the parameters that are used for running them.
    a) Permissions - incorrect and excessive allocation of privileges to running containers.
    b) Ports - unreasonably opened network ports.
    c) Volumes - unsafe use of shared volumes.
5. **Docker image repository** – all issues related to securing storage and delivery of images from our repository to the target system. These can be Docker Hub, third party or local repositories.
6. **Docker distributed systems** - all problems related to distributed deployment of containers and ensuring the security of systems that manage this deployment.
7. **Docker container monitoring** - measures that allow to quickly monitor the status of running containers and act accordingly in case of abnormal behavior of certain parameters.
8. **Docker data backup** - measures to organize the protection of stored data created and used in the process of running applications in containers.

Attacking surface – Docker escape as an example of well-known exploit

A team of information security analysts from Project Zero discovered this vulnerability in July 2019. Despite the fact that it's been more than two years, containers can still be exploited this way. There is no mention of this vulnerability either in the official Docker blog or in the Docker forum [4].

The one can perform escape from the Docker container when it is runs in privileged mode. The flag `--privileged` is used to run privileged containers, known as allowing root access to the host operating system. The one can also escape when the container is started with the `--cap-add` option and the `SYS_ADMIN` privilege is given as a parameter. The `--cap-add` option allows to specify certain privileges (Linux capabilities). The `SYS_ADMIN` privilege grants permission to execute commands such as `quotactl`, `mount`, `umount`, `swapon`, `swapoff`, `sethostname`, and `setdomainname`.

To prevent the system from being compromised this way, one must follow these rules:

1) Do not run containers with the `--privileged` flag.
2) Do not run containers with the `SYS_ADMIN` privilege.
3) Do not use the root account inside the container.
4) Use the file system inside the container in read-only mode (`--read-only = true` option) [5].

Summary

The growth of popularity of Docker and containerization technology is unprecedented - exponential with no plateau seen in sight. At the same time, Linux OS, and its containers in particular, are not immune to various security risks. It does not matter if the breaches and exploits are left accidentally, because of

lack of knowledge, or for purpose – every user should be aware of the main aspects and basic security rules of behaving with Docker to avoid deplorable consequences.

In a further Bachelor's Thesis, more vulnerabilities will be investigated, including methods of their discovery, analysis, and prevention.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Stack Overflow Annual Developer Survey 2021 [Електронний ресурс] // StackOwerflow. – 2022. – Режим доступу до ресурсу: https://insights.stackoverflow.com/survey/2021.
2. Red_Kangaroo.pdf [Електронний ресурс] // Prevasio. – 2022. Режим доступу до ресурсу: https://knowledge-base.prevasio.io/pdf.html?file=Red_Kangaroo.pdf
3. Key Security Layers of Docker Containers – Mohit Vaish [Електронний ресурс] // LinkedIn. – 2022. Режим доступу до ресурсу: https://www.linkedin.com/pulse/key-security-layers-docker-containers-mohit-vaish/?articleId=6618475728398835713
4. Docker – Container Escape – Linux local exploit [Електронний ресурс] // Exploit Database – 2022. Режим доступу до ресурсу: https://www.exploit-db.com/exploits/47147
5. Understanding Docker container escapes [Електронний ресурс] // Trail of bits blog. – 2022. Режим доступу до ресурсу: https://blog.trailofbits.com/2019/07/19/understanding-docker-container-escapes/

Гураль Катерина Володимирівна *— студентка групи 1БС-20мс, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: k.gural@outlook.com*

Науковий керівник: ***Войтович Олеся Петрівна*** *— кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця e-mail: voytovych.op@gmail.com*

Hural Kateryna Volodymyrivna *— student of the group 1BS-20ms, Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: k.gural@outlook.com*

Supervisor: ***Voytovych Olesia Petrivna*** *— Candidate of Technical Sciences (Ph.D.), Associate Professor at the Department of Information protection, Vinnytsia National Technical University, Vinnytsia, e-mail: voytovych.op@gmail.com*