

ТЕСТУВАННЯ ТА АНАЛІЗ РИЗИКІВ БЕЗПЕКИ КОНТЕЙНЕРІВ НА ОСНОВІ DOCKER

Федюшин О.І., Мороз А.В.

Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянуті вразливості та ризики при використанні контейнерів на основі Docker.

Об'єктом дослідження є використання контейнерів на базі Docker, що зараз є одним із найпоширеніших типів. Предмет дослідження – тестування на вразливості контейнерів на основі Docker [1, 2].

При порівнянні звичайної технології віртуалізації та технології контейнерів Docker - основна різниця в технологіях, на яких базується Docker, а саме namespaces та cgroups, що включає ізоляції процесів, файлової системи, пристроїв, між процесною взаємодії, мережі та обмеження ресурсів.

У середовищі Docker, кожен контейнер використовує ядро операційної системи, а сам контейнер є лише кілька процесів, запущених на host системі. Його безпека, особливо ізоляція, теоретично і практично відрізняється від традиційних віртуальних машин.

В результаті дослідження виявлено, що в порівнянні з технологією віртуалізації, контейнерна технологія Docker відрізняється гнучкістю і легкою вагою, і вона незамінна при просуванні хмарних додатків. Але прагнення високої ефективності приводить до втрати повної ізоляції. З точки зору безпеки маємо багато недоліків у порівнянні з технологією віртуалізації, а саме захист зображень контейнерів, безпека ядра, безпека мережі, безпека віртуалізації, безпека під час виконання та інші аспекти.

Для усунення недоліків в роботі з точки зору безпеки потрібно розглядати основні вектори атак, виходячи з яких можна запропонувати методи захисту [3, 4] (контроль доступу, ізоляція та обмеження ресурсів, сканування образів, моніторинг контейнерів, захист при передачі образів, аудит безпеки, контроль мережі та інші) та їх реалізації. Для моделювання атак було розгорнуто тестове середовище, оцінені потенційні вразливості та ризики безпеки. Основна ідея – автоматизація тестування за допомогою програмних засобів.

Список літератури

1. CVE -search results. CVE -CVE. URL: <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=docker> (дата звернення: 05.11.2022).
2. Docker: accelerated, containerized application development. Docker. URL: <https://www.docker.com/> (дата звернення: 05.11.2022).
3. Kubernetes. Kubernetes. URL: <http://kubernetes.com/> (дата звернення: 05.11.2022).
4. Безопасность Docker. Защита инфраструктуры на Docker. TECH GEEK. URL: <https://tech-geek.ru/docker-security/> (дата звернення: 05.11.2022).