Секція 1

ДОСЛІДЖЕННЯ ІНСТРУМЕНТІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ DOCKER-КОНТЕЙНЕРІВ

Юдін О. В.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Цуранов М. В.

Актуальність. З розвитком хмарних технологій, ціна на зберігання та обслуговування даних істотно зменшилась [1]. Що призвело до стрімкого росту використання послуг хмарних провайдерів бізнесом. Для зменшення витрат ресурсів у хмарному сховищі, розробники почали використовувати технологію контейнеризації. Контейнер – це стандартна одиниця ПЗ, яка упаковує код та всі його модулі, тому додаток швидко і надійно переміщається з одного обчислювального середовища в інше [2]. Серед багатьох ПЗ для контейнеризації, 36 % ринку займає «Docker», станом на 2021 рік, це найбільший відсоток використання для ПЗ з контейнеризації [3]. Однак, через зріст попиту на хмарну інфраструктуру, дана галузь привернула увагу зловмисників, які в тому числі намагаються отримати доступ до керуючої машини через вразливості «Docker». У своєму звіті компанія Aqua Security стверджує, що 50% нових неправильно налаштованих екземплярів Docker піддаються атакам ботнетів протягом 56 хвилин після установки [4]. Статистичні дані збираються за допомогою сканерів вразливостей, які не тільки сканують контейнер на предмет безпечності його використання, а й відправляють статистику вразливостей на сервер, для формування аналітики.

Метою даної роботи є дослідження безпеки сучасних Docker-контейнерів.

Аналізуючи ринок хмарних технологій, дослідники компанії Trend Micro виявили новий шифрувальник DarkRadiation. Дане шкідливе ПЗ є bash-скриптом, та призначене для ураження серверної частини Docker контейнерів, які розташовані на дистрибутивах Red Hat, CentOS. Шкідливий скрипт, має змогу зупинити або відключити всі запущені Docker-контейнери. Способом поширення вірусу є скомпрометовані облікові записи та втрачені SSH-ключі [5].

Основні положення. Для своєчасного виявлення НСД до контейнера, використовуються два типи сканерів вразливостей: статичні та динамічні. Серед статичних сканерів, ефективним є Anchore, це утиліта для перевірки наявності вразливостей в образі по базі «CVE». При перевірці контейнера, утиліта сканує відкриті порти, конфігурацію екземпляра. База CVE – є

одною з найбільших баз вразливостей в комп'ютерної мережі. В роботі розглянуто переваги та недоліки сканерів вразливостей для ПЗ контейнеризації.

Висновки. Програмне забезпечення «Docker» є невід'ємною частиною DevOps-технології та має багатогранні інструменти захисту. Однак, більшість інструментів не інстальовані за замовчуванням. Більшість розробників не орієнтовані на безпечну конфігурацію контейнеру. На практиці, це відбувається через брак знань розробників та адміністраторів. Зменшити ризик НСД до чутливих об'єктів можна за допомогою сканерів вразливостей, однак даний метод є лише емпіричним тестом безпеки і не гарантує безпечність екземпляра.

Список літератури

1. Савчук В. О., Цуранов М. В. Аналіз засобів безпеки хмарних платформ. У кн.: Проблеми інформатизації: тези доп. 8-ї міжнар. наук.-техн. конф., 26-27 листопада 2020 р., м. Черкаси, м. Харків, м. Баку, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Черк. держ. технолог. ун-т [та ін.]. – Харків : Петров В. В., 2020. – 83 с.;
2. Use containers to Build, Share and Run your applications. *Docker*. URL – https://www.docker.com/resources/what-container (дата звернення: 17.10.2021);
3. Sysdig 2021 container security and usage report. *Sysdig*. URL – https://sysdig.com/blog/sysdig-2021-container-security-usage-report/ (дата звернення: 29.02.2021);
4. Aqua Security protects containerized apps and infrastructure, raises $135M. *Venture Beat*. URL – https://venturebeat.com/2021/03/10/aqua-security-protects-containerized-apps-and-infrastructure-raises-135m/ (дата звернення: 18.10.2021);
5. Актуальные киберугрозы: II квартал 2021 года. *Positive Technologies*. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q2/ (дата звернення: 18.10.2021).

Відомості про авторів

Юдін Олесь Вікторович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 066-554-94-07, o.yudin@student.csn.khai.edu

Цуранов Михайло Віталійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, m.tsurabov@csn.khai.edu