Секція 1

# АНАЛІЗ ЗАГРОЗ ПЛАТФОРМИ DOCKER В УМОВАХ СУЧАСНОЇ КОНТЕЙНЕРИЗАЦІЇ

Лобойко І. Є.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Землянко Г. А.

**Актуальність.** Контейнеризація стала ключовою складовою сучасних IT-систем, а Docker – однією з найпопулярніших платформ для її впровадження [1]. Контейнери Docker забезпечують однакове виконання коду незалежно від платформи, завдяки чому більшість розробників обирає їх для реалізації проектів [2].

Дослідження безпеки Docker стає особливо актуальним з ростом його популярності, що з часом буде приваблювати все більше зловмисників. Хоча в платформі Docker за час її існування було знайдено понад 37 вразливостей, головна небезпека надходить від контейнерів, вони не є ізольованими і можуть мати додаткові адміністративні привілеї [3].

**Метою** даної роботи є аналіз загроз платформи Docker у контексті сучасної контейнеризації. Також будуть розроблені рекомендації для підвищення рівня захисту під час використання даної платформи.

**Основні положення.** У рамках дослідження було виявлено кілька серйозних вразливостей платформи Docker, що безпосередньо пов’язані з її архітектурою та взаємозв'язком з хост-системою. Серед них [4]: Втеча з контейнера (CVE-2019-5736) – вразливість, що дозволяє зловмиснику перезаписати бінарний файл runc на хост-системі, отримуючи root-доступ і загрожуючи інфраструктурі. «Брудна труба» (CVE-2022-0847) – недолік у конвеєрі ядра, що дозволяє змінювати файли без доступу та підвищувати привілеї, загрожуючи конфіденційності даних. Неконтрольоване споживання ресурсів (CVE-2021-21285) – вразливість, що викликає аварійне завершення роботи демона Docker через неправильно сформований маніфест, що може призвести до відмови в обслуговуванні. Обхід каталогу (CVE-2014-9356) – вразливість, що надає доступ до чутливих файлів, загрожуючи безпеці контейнеризованих застосунків. Неправильна ініціалізація (CVE-2019-14271) – вразливість, що дозволяє ін’єкцію коду через динамічне завантаження бібліотек у середовищі chroot, підвищуючи ризик зловмисного втручання. Для запобігання вразливостям важливо слідкувати за оновленнями платформи Docker, завантажувати образи тільки з перевірених джерел і регулярно сканувати контейнери

додатковим ПЗ. Прикладом такого програмного забезпечення є Docker Bench [5]. Крім цього, слід дотримуватись наступних порад: уникати використання користувача root, обмежувати системні ресурси та kernel capabilities, а також налаштувати мінімальне середовище, щоб зменшити вектор атаки.

**Висновки.** Головна загроза при використанні Docker надходить від контейнерів, тому варто вживати заходів для забезпечення їх безпеки, зокрема використовувати непривілейованих користувачів, налаштувати мінімальне середовище та сканувати контейнери на наявність вразливостей або помилок конфігурації. Крім цього, можна вимкнути icc (inter-container connectivity) або запускати контейнери з read-only файловою системою.

**Список літератури**

1. Best Container Engine Software. *G2*. URL – https://www.g2.com/categories/container-engine (дата звернення: 31.10.2024).
2. Docker's 2024 State of Application Development Report Highlights Key Trends for Developers. *ADTmag*. URL – https://adtmag.com/Articles/2024/06/12/Docker-2024-State-of-AppDev-Report.aspx (дата звернення: 31.10.2024).
3. Docker Docker security vulnerabilities, CVEs, versions and CVE reports. *CVE security vulnerability database*. URL – https://www.cvedetails.com/product/28125/Docker-Docker.html?vendor_id=13534 (дата звернення: 31.10.2024).
4. Top 5 docker security vulnerabilities in 2023. *Snyk*. URL – https://snyk.io/learn/docker-security/top-5-vulnerabilities (дата звернення: 31.10.2024).
5. Docker Bench for Security. GitHub. URL: https://github.com/docker/docker-bench-security (дата звернення: 31.10.2024).

**Відомості про авторів**

Лобойко Ілля Євгенович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», i.loboiko@student.csn.khai.edu
Землянко Георгій Андрійович, ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», PhD з кібербезпеки, g.zemlynko@csn.khai.edu