Ткачук М.А., магістрант
Кузьменко О.В., ст. викладач
Державний університет «Житомирська політехніка»

АНАЛІЗ МЕТОДІВ АТАК НА DOCKER-КОНТЕЙНЕРИ ТА ПІДХОДІВ ДО ЇХ ЗАХИСТУ

У контексті сучасних кіберзагроз Docker-контейнери, як одна з провідних технологій контейнеризації, залишаються важливою ціллю для кіберзлочинців. Атаки на Docker-контейнери можуть призводити до компрометації інфраструктури, тому аналіз методів атак і механізмів захисту має вирішальне значення для забезпечення безпеки.

У ході дослідження класифіковано основні методи атак на Docker-контейнери. Одним із ключових напрямів є атаки на образи контейнерів через вразливості в публічних репозиторіях. Зловмисники можуть вбудовувати шкідливий код у популярні образи, що призводить до зараження під час їх використання [1].

Другий напрямок атак включає компрометацію конфігурацій. Використання невірно налаштованих Docker-файлів або привілеїв "root" у контейнерах значно підвищує ризик експлуатації [2]. Особливо небезпечними є атаки на Docker API, який у разі відкритого доступу може стати шлюзом до всієї інфраструктури [3].

Ще одним важливим методом атак є використання механізмів міжконтейнерної взаємодії. Експлуатація незахищених мережевих з'єднань між контейнерами дозволяє зловмисникам поширювати атаку на інші сервіси у кластері [4].

Дослідження також розглянуло вплив людського фактора. Недотримання найкращих практик безпеки, таких як недокументовані паролі або відсутність обмеження доступу, сприяє успішним атакам [5].

Аналіз методів захисту показав, що регулярне оновлення Docker-образів і впровадження політик безпеки для Docker API значно знижують ризики атак [6]. Впровадження інструментів, таких як Docker Bench for Security, дозволяє автоматизувати процес аудиту. Крім того, ізоляція контейнерів із використанням технологій, як-от SELinux або AppArmor, додає рівень захисту [7].

Таким чином, результати дослідження підкреслюють необхідність комплексного підходу до безпеки Docker-контейнерів, який включає: регулярний аудит конфігурацій, моніторинг аномальної активності та впровадження політик обмеження привілеїв. Розроблені рекомендації можуть бути адаптовані для різних організацій та відповідають сучасним стандартам кібербезпеки.

Список використаних джерел

1. Docker Security Scanning: What It Is and Why You Need It [Електронний ресурс] / Docker Official Blog. – 2023. – URL: https://www.docker.com/blog/security-scanning
2. Best Practices for Writing Dockerfiles [Електронний ресурс] / Docker Documentation. – 2024. – URL: https://docs.docker.com/develop/develop-images/dockerfile_best-practices/
3. Understanding Docker API Security [Електронний ресурс] / Palo Alto Networks. – 2023. – URL: https://unit42.paloaltonetworks.com/docker-api-security/
4. Container Networking Security: Best Practices [Електронний ресурс] / Aqua Security. – 2024. – URL: https://www.aquasec.com/container-networking-security/
5. Human Factor in Cybersecurity: Addressing the Weakest Link [Електронний ресурс] / ScienceDirect. – 2023. – URL: https://www.sciencedirect.com/article/human-factor-in-cybersecurity
6. Securing Docker API: Strategies and Tools [Електронний ресурс] / Check Point. – 2023. – URL: https://www.checkpoint.com/securing-docker-api
7. SELinux and AppArmor for Container Security [Електронний ресурс] / Red Hat. – 2023. – URL: https://www.redhat.com/en/technologies/linux-platforms/security-selinux-apparmor