Методы обеспечения безопасности при работе с Docker

М.А. Копашенко, И.С. Позняк

Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия

Обоснование. Docker — это мощная платформа для упаковки и запуска приложений в изолированных средах, которая может помочь обеспечить безопасность основной машины. Однако по умолчанию контейнеры не полностью безопасны, и необходимо использовать настройки безопасности для минимизации угроз. При создании контейнера необходимо использовать некоторые настройки безопасности, которые в будущем усложнят жизнь злоумышленнику.

Цель — вывести основные методы, которые помогут улучшить безопасность контейнеров и предотвратить возможные атаки.

Методы.

1. Установить лимит ресурсов доступных контейнеру, чтобы защититься от атак типа DDoS, которые могут заставить контейнер максимально загрузить ЦП.

Пример опции для ограничения использования ЦП четырьмя ядрами: --cpuset-cpus="0-3"

2. Использовать непривилегированного пользователя внутри контейнера. Docker по умолчанию в каждом контейнере использует пользователя root с максимальными правами, что может упростить дальнейшее продвижение для злоумышленников [1].

3. Ввести запрет на повышение привилегий пользователей внутри контейнера, это позволит предотвратить повышения привилегий в контейнере путем использования setuid и setgid путем добавления опции: --security-opt=no-new-privileges

4. Не предоставлять доступ к UNIX-сокету Docker. При получении доступа к сокету злоумышленник сможет получить root права, связаться с операционной системой хоста и контролировать ее.

5. Использовать в качестве образов, на которых основаны контейнеры, легковесные образы заранее проверенных издателем систем, с минимальным числом компонентов.

Результаты. Применив данные методы, можно достичь увеличение уровня безопасности Docker-контейнеров. Были уменьшены возможности атак с использованием повышения привилегий пользователей и атак типа DDoS, а также был предотвращен доступ к UNIX-сокету Docker. Использование легковесных образов также помогло уменьшить количество возможных уязвимостей. В целом применение данных методов позволяет достичь более высокого уровня безопасности в среде Docker, что, в свою очередь, может уменьшить риск потенциальных угроз для приложений и данных, работающих в контейнерах.

Выводы. В данной статье было рассмотрено несколько методов, которые помогут защитить контейнеры. Несмотря на то, что компания Docker уже предоставляет контейнеры с минимальным количеством возможностей, все еще остаются потенциальные векторы атак [2]. Для реализации защиты используется правило уменьшения количества привилегий контейнера, выдаваемых ему по умолчанию.

Ключевые слова: контейнер; безопасность; веб приложения; Docker; методы; атаки.

Список литературы

1. docs.docker.com [Электронный ресурс]. Isolate containers with a user namespace. Доступ по: https://docs.docker.com/engine/security/userns-remap/
2. medium.com [Электронный ресурс]. On the security of containers. Доступ по: https://medium.com/@ewindisch/on-the-security-of-containers-2c60ffe25a9e

Сведения об авторах:

Михаил Алексеевич Копашенко — студент, группа ИБТС-01, факультет кибербезопасности и управления (факультет № 1); Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия. E-mail: mikop63@gmail.com

Ирина Сергеевна Позняк — научный руководитель, доцент кафедры информационная безопасность; Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия. E-mail: i.pozdnyak@psuti.ru