Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.45

Забавский
Владислав Владимирович

Методика обнаружения уязвимостей в контейнерах Docker

АВТОРЕФЕРАТ
магистерской диссертации на соискание степени магистра
по специальности 1-98 80 01 Информационная безопасность

_____

Научный руководитель
Борботько Тимофей Валентинович,
доктор технических наук, профессор

_____

Минск 2021

ВВЕДЕНИЕ

Рассматривая проблему уязвимостей в технологии контейнеризации Docker, невозможно не затронуть концепцию монолитной и микросервисной архитектуры систем. В монолитные системы, со временем, довольно сложно внедрять новые элементы, например: использовать другой язык программирования или базу данных. При отказе работы такой системы, откажет работать весь сервис, а если нужно внести изменение в одну строку монолитного приложения, состоящего из миллиона строк кода, требуется чтобы было развернуто все приложение. В отличии от монолитного приложения, которое является одним целым, микросервисное приложение разбито на небольшие, автономные, совместно работающие сервисы. Такая архитектура дает следующие преимущества: можно использовать внутри каждого из сервисов различные технологии; при отказе одного из компонентов системы, проблему можно изолировать, сохранив работоспособность всей системы; можно вносить изменения в отдельный микросервис и развертывать его независимо от остальной системы. Микросервисы являются современным и новым подходом к построению архитектуры сервисов. Поэтому многие крупные организации, такие как Amazon, Google и Netflix используют их в построении своих систем [1].

Технология контейнеризации Docker является основой построения микросервисных приложений. Это приложение может состоять из нескольких десятков, а иногда, и тысяч контейнеров Docker. Docker – это программное обеспечение, основная задача которого – контейнеризация сервисов. Этот тип виртуализации позволяет упаковывать программное обеспечение в контейнеры. Контейнер имеет некоторое сходство с виртуальной машиной, которая может быть использована, чтобы содержать и выполнять требуемое программное обеспечение, необходимое для запуска определенной программы или набора программ [2].

Микросервисная архитектура, и как следствие, Docker получают все большее распространение в мире, поэтому технология контейнеризации с каждым днем привлекает все больше злоумышленников [3] [4] [5]. Согласно отчету «Sysdig 2021 Container Security and Usage Report» [6], исследователями были случайно выбраны и просканированы образы контейнеров. По результатам исследований, 55% образов контейнеров не прошли сканирование, так как содержат в себе известные уязвимости со

значением «Высокая степень опасности» или выше. Среди всех отсканированных образов контейнеров, больше всего уязвимостей высокого или критического уровня тяжести последствий было найдено в тех контейнерах, которые представляют собой дополнительные библиотеки или сервисы – 53 %, а в образах контейнеров с операционными системами – 4%. Несмотря на то, что многие организации понимают необходимость сканирования на наличие уязвимостей, они могут не проверять на наличие распространенных ошибок конфигурации. Из отчета следует, что 58% образов контейнеров запускаются с правами «root», что позволяет использовать привилегированные контейнеры, которые могут быть скомпрометированы.

Создание системы, которая бы выполняла сканирование, и обнаружение известных уязвимостей в технологии контейнеризации Docker считаю своевременным и актуальным. Такая система могла бы предотвратить выпуск продукта компании с уязвимостями в производственную среду.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научной, научно-технической и инновационной деятельности

Тема диссертационной работы соответствует разделу 6 «Обеспечение безопасности человека, общества и государства» приоритетных направлений научной, научно-технической и инновационной деятельности в Республики Беларусь на 2021–2025 гг., утверждённых Указом Президента Республики Беларусь 7 мая 2020 г., № 156. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке последовательности процессов, обеспечивающих выявление уязвимостей приложений, заключенных в контейнерах Docker.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Проанализировать архитектуру технологии контейнеризации Docker.
2. Проанализировать уязвимости технологии контейнеризации Docker.
3. Разработать систему, которая бы выполняла сканирование, и обнаружение известных уязвимостей в технологии контейнеризации Docker.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на XVII Международной научно-практической конференции «Управление информационными ресурсами» (Минск, 2021).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 1 работа, в том числе 1 статья в сборниках материалов конференций.

Личный вклад соискателя

Все основные результаты, изложенные в диссертационной работе, получены соискателем самостоятельно. Разработанная система для сканирования и обнаружения известных уязвимостей в технологии контейнеризации Docker является полностью собранной и настроенной и не

требует от пользователей подробного знания деталей. В то же время, ее можно модифицировать и менять настройки по собственному усмотрению. Применяться система может в любой организации, использующей микросервисную архитектуру для построения своих приложений.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, трех глав, заключения и библиографического списка. Общий объем диссертации 93 страницы, 44 наименования в библиографическом списке.

Во введение приводится обоснование актуальности работы.

Первая глава носит обзорный характер. В ней приводится общее описание технологии контейнеризации Docker, а именно архитектура Docker и последовательность процессов, обеспечивающих инсталляцию приложения из контейнера Docker

Вторая глава посвящена уязвимостям контейнеров Docker. Затрагиваются такие проблемы как уязвимости конфигурации Docker и получение привилегий, обеспечивающих выход за пределы контейнера Docker. Так же приведены методы и средства обнаружения уязвимостей в контейнерах Docker

В третьей главе описывается методика обнаружения уязвимостей в контейнерах Docker. Для реализации данной методики была построена система, которая использует инструмент непрерывной интеграции Jenkins, программное обеспечение для сканирования образов Docker контейнеров – Anchore Engine и хранилище Nexus 3.

Как результат работы системы, в конце публикуется детальный отчет, из которого следует: можно ли использовать просканированный образ Docker контейнера, и если он отмечен как «SUCCESS», то данный образ можно использовать. Если же отчет помечен как «FAILED», то в этом образе нужно устранять уязвимости.

Разработанная система является полностью собранной и настроенной и не требует от пользователей детального знания деталей. В то же время, ее можно модифицировать и менять настройки по собственному усмотрению. Применяться система может в любой организации, использующей микросервисную архитектуру для построения своих приложений.

В заключении сформулированы основные результаты диссертации.

ЗАКЛЮЧЕНИЕ

Контейнеры помогают людям создавать более безопасные среды, поскольку они изолируют программное обеспечение. Однако использование контейнеров также увеличивает область атак и рисков, поскольку программное обеспечение для контейнеризации также добавляет дополнительные уровни абстракции и сложности. Это создает проблемы как для злоумышленников, так и для защитников систем Docker.

При разработке или обслуживании системы, использующей Docker, важно помнить о следующих моментах:

1. Ошибки в конфигурации Docker могут предоставлять больший интерес для злоумышленника, чем программные ошибки, связанные с безопасностью, потому что неправильную конфигурацию сложнее исправить. Программные ошибки легко исправить, используя последнюю версию Docker, в то время как для исправления неправильной конфигурации потребуются изменения способа использования Docker;

2. Docker, как и все программы для контейнеризации, добавляет уровень изоляции. Это повышает безопасность, поскольку программное обеспечение изолировано от основной системы. Однако это также добавляет уровень абстракции к системе. Вместо того чтобы запускать программное обеспечение непосредственно на хосте, оно запускается внутри контейнера на хосте. Этот уровень абстракции увеличивает область атак на систему;

3. Существует множество уязвимостей, представляющих опасность для систем, использующих Docker. Можно значительно снизить риск ошибок в программном обеспечении, если всегда использовать последнюю версию Docker;

4. Не стоит полагаться только на списки рекомендаций. Они (например, CIS Docker Benchmark) являются хорошей отправной точкой для укрепления системы. Однако списки рекомендаций не являются исчерпывающими;

5. Использовать программное обеспечение для анализа образов Docker. Такие программы полезны, поскольку экономят время и систематически изучают целевые системы. Методика обнаружения уязвимостей в контейнерах Docker, разработанная в данной работе, является примером такой программы. Эта система является полностью собранной и настроенной

и не требует от пользователей детального знания деталей. В то же время, ее можно модифицировать и менять настройки по собственному усмотрению. Применяться система может в любой организации, использующей микросервисную архитектуру для построения своих приложений.

Использование перечисленных пунктов станет отправной точкой для создания более безопасной инфраструктуры в области, касающейся контейнеризации.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1-А. Забавский В.В. Уязвимости в технологии контейнеризации Docker /В.В. Забавский, Т.В. Борботько // 17 международная научно-практическая конференция «Управление информационными ресурсами» Материалы 17 межд. Науч.-практич. конф., Минск, 12 марта 2021 г. - Минск: УО «Академия управления при Президенте Республики Беларусь», 2021. - С.208-209.