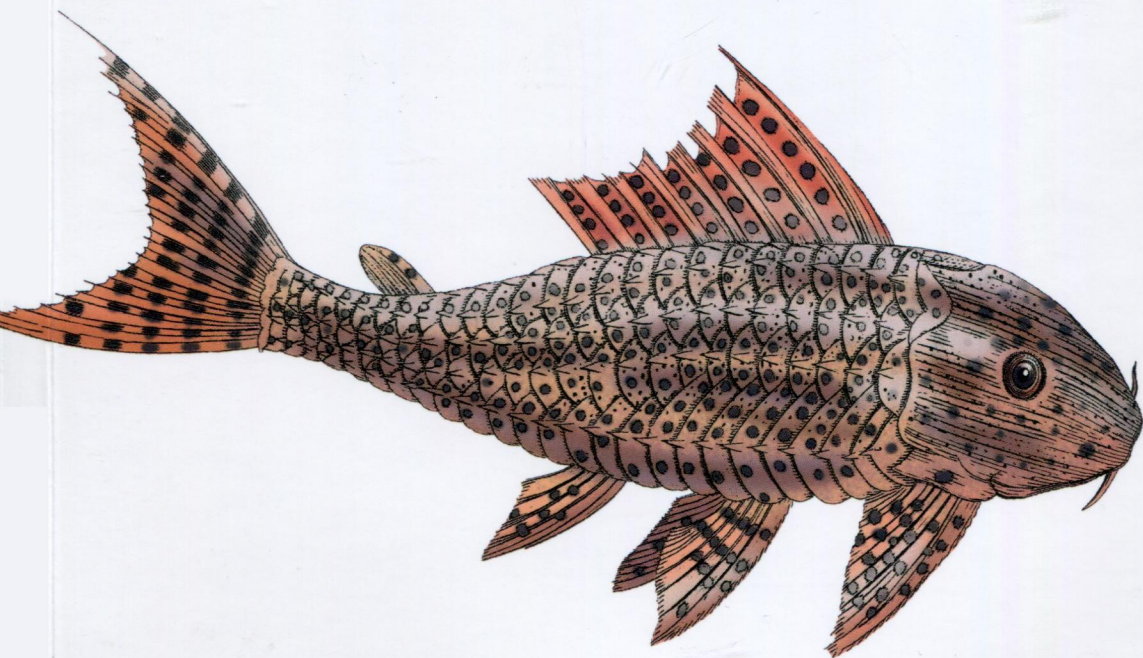


O'REILLY®

Безопасность контейнеров

Фундаментальный подход к защите
контейнеризированных приложений



Лиз Райс

Безопасность контейнеров

Фундаментальный подход к защите
контейнеризированных приложений

Лиз Райс



Санкт-Петербург · Москва · Минск

2021

ББК 32.988.02-018-07
УДК 004.056.53
Р18

Райс Лиз

Р18 Безопасность контейнеров. Фундаментальный подход к защите контейнеризированных приложений. — СПб.: Питер, 2021. — 224 с.: ил. — (Серия «Бестселлеры O'Reilly»).

ISBN 978-5-4461-1850-2

Во многих организациях приложения работают в облачных средах, обеспечивая масштабируемость и отказоустойчивость с помощью контейнеров и средств координации. Но достаточно ли защищена развернутая система? В этой книге, предназначенной для специалистов-практиков, изучаются ключевые технологии, с помощью которых разработчики и специалисты по защите данных могут оценить риски для безопасности и выбрать подходящие решения.

Лиз Райс исследует вопросы построения контейнерных систем в Linux. Узнайте, что происходит при развертывании контейнеров, и научитесь оценивать возможные риски для безопасности развертываемой системы. Приступайте, если используете Kubernetes или Docker и знаете базовые команды Linux.

16+ (В соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ.)

ББК 32.988.02-018-07
УДК 004.056.53

Права на издание получены по соглашению с O'Reilly. Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав.

Информация, содержащаяся в данной книге, получена из источников, рассматриваемых издательством как надежные. Тем не менее, имея в виду возможные человеческие или технические ошибки, издательство не может гарантировать абсолютную точность и полноту приводимых сведений и не несет ответственности за возможные ошибки, связанные с использованием книги. Издательство не несет ответственности за доступность материалов, ссылки на которые вы можете найти в этой книге. На момент подготовки книги к изданию все ссылки на интернет-ресурсы были действующими.

ISBN 978-1492056706 англ.

Authorized Russian translation of the English edition of Container Security
ISBN 9781492056706 © 2020 Vertical Shift Ltd.

ISBN 978-5-4461-1850-2

This translation is published and sold by permission of O'Reilly Media, Inc., which owns or controls all rights to publish and sell the same.

© Перевод на русский язык ООО Издательство «Питер», 2021

© Издание на русском языке, оформление ООО Издательство «Питер», 2021

© Серия «Бестселлеры O'Reilly», 2021

Краткое содержание

Предисловие	13
Глава 1. Угрозы безопасности контейнеров.....	21
Глава 2. Системные вызовы Linux, права доступа и привилегии	36
Глава 3. Контрольные группы	48
Глава 4. Изоляция контейнеров	57
Глава 5. Виртуальные машины	85
Глава 6. Образы контейнеров.....	97
Глава 7. Программные уязвимости в образах контейнеров	118
Глава 8. Усиление изоляции контейнеров	134
Глава 9. Нарушение изоляции контейнеров	147
Глава 10. Сетевая безопасность контейнеров	162
Глава 11. Защищенное соединение компонентов с помощью TLS.....	180
Глава 12. Передача в контейнеры секретных данных.....	192
Глава 13. Защита контейнеров во время выполнения	201
Глава 14. Контейнеры и десять главных рисков по версии OWASP	210
Заключение	216
Приложение. Контрольный список по безопасности.....	218
Об авторе	221
Об иллюстрации на обложке	222

Оглавление

Предисловие	13
Для кого эта книга	14
Структура издания	15
Примечание относительно Kubernetes	16
Примеры	17
Запуск контейнеров.....	17
Обратная связь.....	18
Условные обозначения	18
Использование примеров кода	19
От издательства	20
Благодарности.....	20
Глава 1. Угрозы безопасности контейнеров	21
Риски, угрозы и уменьшение их последствий.....	22
Модель угроз для контейнеров.....	23
Границы зон безопасности	27
Мультиарендность	28
Совместно используемые машины	29
Виртуализация	30
Мультиарендность контейнеров	31
Экземпляры контейнеров	32
Принципы безопасности	33
Минимум полномочий.....	33
Многослойная защита	33
Минимальная поверхность атаки.....	33

Ограничение радиуса поражения	34
Разграничение обязанностей.....	34
Реализация принципов безопасности с помощью контейнеров	34
Резюме.....	35
Глава 2. Системные вызовы Linux, права доступа и привилегии	36
Системные вызовы	36
Права доступа к файлам.....	38
Биты <code>setuid</code> и <code>setgid</code>	39
Привилегии Linux	44
Повышение полномочий.....	46
Резюме.....	47
Глава 3. Контрольные группы	48
Иерархии контрольных групп	48
Создание контрольных групп.....	50
Установка ограничений на ресурсы	52
Приписываем процесс к контрольной группе.....	53
Контрольные группы в Docker	54
Контрольные группы версии 2.....	55
Резюме.....	56
Глава 4. Изоляция контейнеров	57
Пространства имен Linux	58
Изоляция хост-имени.....	60
Изоляция идентификаторов процессов.....	61
Изменение корневого каталога.....	65
Сочетание возможностей пространств имен и изменения корневого каталога	68
Пространство имен монтирования	69
Пространство имен сети	71
Пространство имен пользователей	74
Пространство имен обмена информацией между процессами.....	77
Пространство имен контрольных групп	78

Процессы контейнера с точки зрения хоста	80
Хост-компьютеры контейнеров	82
Резюме	83
Глава 5. Виртуальные машины	85
Загрузка компьютера	85
Знакомство с VMM	87
VMM Type 1 (гипервизоры)	88
VMM Type 2	89
Виртуальные машины, работающие в ядре	90
«Перехватывай и эмулируй»	91
Обработка не виртуализируемых инструкций	92
Изоляция процессов и безопасность	93
Недостатки виртуальных машин	94
Изоляция контейнеров по сравнению с изоляцией виртуальных машин	95
Резюме	96
Глава 6. Образы контейнеров	97
Корневая файловая система и конфигурация образов контейнеров	97
Переопределение настроек во время выполнения	98
Стандарты ОСI	99
Конфигурация образа	100
Сборка образов	101
Опасности команды <code>docker build</code>	101
Сборка без использования демона	102
Слои образов	103
Хранение образов	105
Идентификация образов	106
Безопасность образов	107
Безопасность этапа сборки	108
Происхождение <code>Dockerfile</code>	108
Практические рекомендации по безопасности <code>Dockerfile</code>	109
Атаки на машину сборки	112

Глава 8. Усиление изоляции контейнеров	134
Механизм seccomp.....	134
Модуль AppArmor	137
Модуль SELinux.....	138
«Песочница» gVisor	140
Среда выполнения контейнеров Kata Containers	144
Виртуальная машина Firecracker	144
Unikernels	145
Резюме.....	146
Глава 9. Нарушение изоляции контейнеров	147
Выполнение контейнеров по умолчанию от имени суперпользователя	147
Переопределение идентификатора пользователя.....	149
Требование выполнения от имени суперпользователя внутри контейнера	150
Контейнеры, не требующие полномочий суперпользователя.....	152
Флаг --privileged и привилегии.....	155
Монтирование каталогов с конфиденциальными данными.....	157
Монтирование сокета Docker	158
Совместное использование пространств имен контейнером и его хостом	159
Вспомогательные контейнеры	160
Резюме.....	161
Глава 10. Сетевая безопасность контейнеров	162
Брандмауэры для контейнеров	162
Сетевая модель OSI.....	164
Отправка IP-пакета	166
IP-адреса контейнеров	168
Сетевая изоляция.....	169
Маршрутизация на уровнях 3/4 и правила.....	169
Утилита iptables.....	170
IPVS	172

Сетевые стратегии.....	173
Программные решения для сетевых стратегий	175
Практические рекомендации для сетевых стратегий	176
Service mesh	177
Резюме.....	179
Глава 11. Защищенное соединение компонентов с помощью TLS.....	180
Защищенные соединения	181
Сертификаты X.509	182
Пары «открытый/секретный ключ»	183
Центры сертификации.....	184
Запросы на подписание сертификатов	186
TLS-соединения	187
Защищенные соединения между контейнерами	189
Отзыв сертификатов.....	190
Резюме	191
Глава 12. Передача в контейнеры секретных данных.....	192
Свойства секретных данных	192
Передача информации в контейнер.....	194
Хранение секретных данных в образе контейнера.....	194
Передача секретных данных по сети	195
Передача секретных данных в переменных среды.....	195
Передача секретных данных через файлы.....	197
Секретные данные в Kubernetes	197
Секретные данные доступны для суперпользователя хоста	199
Резюме	200
Глава 13. Защита контейнеров во время выполнения	201
Профили образов контейнеров.....	201
Профили сетевого трафика	202
Профили исполняемых файлов	202
Профили доступа к файлам.....	204

Профили идентификаторов пользователей	205
Другие профили времени выполнения	205
Утилиты обеспечения безопасности контейнеров	206
Предотвращение отклонений	208
Резюме	209
Глава 14. Контейнеры и десять главных рисков по версии OWASP	210
Внедрение кода	210
Взлом аутентификации	210
Раскрытие конфиденциальных данных	211
Внешние сущности XML	211
Взлом управления доступом	212
Неправильные настройки безопасности	212
Межсайтовое выполнение сценариев (XSS)	213
Небезопасная десериализация	213
Использование компонентов, содержащих известные уязвимости	214
Недостаток журналирования и мониторинга	214
Резюме	215
Заключение	216
Приложение. Контрольный список по безопасности	218
Об авторе	221
Об иллюстрации на обложке	222