

УДК 004.451  
ББК 32.972.1  
В34

**Вермейлен С.**

**В34** Администрирование системы защиты SELinux / пер. с англ. В. Л. Верещагина, О. К. Севостьяновой. – М.: ДМК Пресс, 2020. – 300 с.: ил.

**ISBN 978-5-97060-557-8**

Эта книга показывает, как значительно усилить безопасность операционной системы Linux и устранить имеющиеся уязвимости установленных приложений.

Вы узнаете, как работает SELinux, как можно настроить ее под свои нужды и усилить с ее помощью защиту систем виртуализации, включающих технологию libvirt (sVirt) и контейнеризацию Docker. Также рассказывается об управляющих действиях, позволяющих улучшить безопасность конкретной системы с помощью принудительного контроля доступа – стратегии защиты, определяющей безопасность Linux уже много лет. Большинство возможностей системы защиты рассматривается на реальных примерах.

Книга предназначена для администраторов операционной системы Linux, в задачу которых входит управление ее защищенностью.

УДК 004.451  
ББК 32.972.1

Authorized Russian translation of the English edition of SELinux System Administration ISBN 978-1-78712-695-4 © Packt Publishing.

This translation is published and sold by permission of Packt Publishing, which owns or controls all rights to publish and sell the same.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-1-78712-695-4 (анг.)

© Packt Publishing

ISBN 978-5-97060-557-8 (рус.)

© Дополнительный текст, Верещагин В. Л., 2020

© Оформление, издание, перевод, ДМК Пресс, 2020

# Содержание

<b>Об авторе .....</b>	<b>13</b>
<b>О рецензентах.....</b>	<b>15</b>
<b>Предисловие .....</b>	<b>16</b>
<b>Глава 1. Фундаментальные концепции SELINUX.....</b>	<b>21</b>
1.1. Предоставление большей безопасности в Linux.....	21
1.1.1. Использование модулей безопасности Linux .....	24
1.1.2. Расширение возможностей стандартного дискреционного разграничения доступа .....	25
1.1.3. Ограничение привилегий пользователя root.....	27
1.1.4. Сокращение воздействия уязвимостей .....	28
1.1.5. Включение возможностей SELinux в операционной системе .....	29
1.2. Маркировка всех ресурсов и объектов .....	31
1.2.1. Описание параметров безопасности.....	32
1.2.2. Принудительный доступ посредством типов функциональных ограничений .....	35
1.2.3. Распределение по ролям наборов функциональных ограничений ....	36
1.2.4. Разделение пользователей по ролям.....	38
1.2.5. Контроль информационных потоков посредством мандатного механизма .....	39
1.3. Формирование и распределение политик .....	40
1.3.1. Создание политик SELinux .....	41
1.3.2. Распределение политик в виде модулей .....	43
1.3.3. Комплектация модулей в хранилище политик.....	45
1.4. Различия между политиками .....	45
1.4.1. Поддержка многоуровневой защиты (MLS) .....	46
1.4.2. Манера поведения с неизвестными разрешениями .....	46
1.4.3. Поддержка неограниченных доменов.....	47
1.4.4. Ограничение межпользовательского обмена .....	48
1.4.5. Последовательные изменения версий политик .....	49
1.4.6. Качественное изменение версий политик.....	50
1.5. Заключение.....	51
<b>Глава 2. Режимы работы и регистрация событий .....</b>	<b>53</b>
2.1. Включение и выключение защиты SELinux .....	53
2.1.1. Установка глобального состояния защиты.....	54

2.1.2. Переключение в рекомендательный и принудительный режимы .....	55
2.1.3. Использование параметров загрузки ядра .....	57
2.1.4. Отключение защиты SELinux для отдельно взятого сервиса.....	58
2.1.5. Определение приложений, активно взаимодействующих с SELinux.....	61
2.2. Регистрация событий и аудит в SELinux.....	61
2.2.1. Последовательность контроля событий о нарушениях безопасности.....	62
2.2.2. Исключение конкретных отказов в доступе из числа регистрируемых.....	64
2.2.3. Конфигурирование подсистемы контроля событий безопасности Linux.....	65
2.2.4. Настройка локального системного регистратора событий.....	66
2.2.5. Разбор информации об отказах SELinux .....	67
2.2.6. Другие типы событий, связанные с SELinux .....	72
2.2.7. Использование команды ausearch .....	76
2.3. Получение помощи при отказах.....	77
2.3.1. Диагностика неисправности с помощью службы setroubleshoot .....	77
2.3.2. Отправка электронной почты, когда случился отказ SELinux .....	80
2.3.3. Использование утилиты audit2why .....	81
2.3.4. Взаимодействие с журналом system.....	82
2.3.5. Использование здравого смысла .....	83
2.4. Заключение.....	85
<b>Глава 3. Управление учетными записями пользователей.....</b>	<b>86</b>
3.1. Параметры безопасности пользователей.....	86
3.1.1. Сложность допустимого набора функций.....	87
3.1.2. Определение неограниченных доменов .....	89
3.2. Пользователи SELinux и их роли.....	90
3.2.1. Перечень сопоставлений пользователей с пользовательскими типами SELinux.....	90
3.2.2. Сопоставление учетных записей с пользовательскими типами .....	92
3.2.3. Настройка учетных записей относительно служб .....	93
3.2.4. Создание типов пользователей SELinux.....	94
3.2.5. Перечень типов допустимого набора функций у ролей.....	95
3.2.6. Управление категориями .....	96
3.3. Управление ролями SELinux.....	98
3.3.1. Настройки присвоения допустимых ролей пользователю .....	98
3.3.2. Проверка параметров безопасности при помощи утилиты getseuser .....	100
3.3.3. Подключение ролей с помощью команды newrole .....	100
3.3.4. Управление доступом к роли с помощью команды sudo .....	101
3.3.5. Переключение параметров безопасности посредством runcon.....	102

3.3.6. Переключение на системную роль .....	102
3.4. SELinux и PAM (подключаемые модули аутентификации) .....	104
3.4.1. Назначение параметров безопасности с помощью подключаемых модулей аутентификации .....	104
3.4.2. Запрещение доступа в рекомендательном режиме работы защиты .....	105
3.4.3. Многоэкземпляльность каталогов .....	106
3.5. Заключение.....	107

## **Глава 4. Домены как допустимые наборы функций**

<b>для процессов и контроль доступа на уровне файлов .....</b>	<b>109</b>
4.1. О параметрах безопасности файлов.....	109
4.1.1. Получение информации о параметрах безопасности.....	110
4.1.2. Интерпретация наименований типов SELinux.....	111
4.2. Закрепление параметров безопасности за объектом и их игнорирование.....	112
4.2.1. Наследование параметров безопасности по умолчанию.....	113
4.2.2. Правила преобразования типов и их вывод .....	113
4.2.3. Копирование и перемещение файлов .....	115
4.2.4. Временное изменение параметров безопасности файла .....	117
4.2.5. Установка категорий для файлов и каталогов .....	118
4.2.6. Использование многоуровневой защиты для файлов .....	118
4.2.7. Резервное копирование и восстановление расширенных атрибутов .....	119
4.2.8. Использование опций монтирования для установки параметров SELinux.....	119
4.3. Формулировка параметров безопасности для файлов .....	121
4.3.1. Использование выражений, описывающих параметры безопасности.....	121
4.3.2. Регистрация изменений параметров безопасности файлов .....	123
4.3.3. Использование заказных типов.....	125
4.3.4. Различные виды файлов file_contexts и их компиляция.....	126
4.3.5. Обмен локальными изменениями.....	127
4.4. Изменение параметров безопасности у файлов.....	127
4.4.1. Использование команд setfiles, rlpkg и fixfiles .....	128
4.4.2. Изменение параметров безопасности на всей файловой системе ...	128
4.4.3. Автоматическое приведение к заданным значениям изменившихся параметров безопасности .....	129
4.5. Параметры безопасности процесса .....	130
4.5.1. Получение параметров безопасности процесса .....	130
4.5.2. Преобразование типа процесса .....	131
4.5.3. Проверка соответствия параметров безопасности .....	133
4.5.4. Другие способы преобразования типов .....	134

4.5.5. Изначально заданные параметры в структуре идентификатора безопасности.....	134
4.6. Определение границ возможных преобразований.....	135
4.6.1. Очистка переменных окружения во время преобразования к другому типу .....	135
4.6.2. Невыполнение преобразований, когда нет ограничивающего родительского типа .....	137
4.6.3. Использование флага, исключающего новые привилегии у процесса.....	138
4.7. Типы, разрешения и ограничения .....	139
4.7.1. Объяснение атрибутов типа .....	139
4.7.2. Запрос разрешений, предоставленных типу процесса.....	140
4.7.3. Рассмотрение наложенных ограничений.....	142
4.8. Заключение.....	143

## **Глава 5. Контроль сетевого взаимодействия..... 144**

5.1. От контроля межпроцессного взаимодействия (IPC) до сокетов базовых протоколов (TCP/UDP) транспортного уровня.....	144
5.1.1. Использование разделяемой памяти .....	145
5.1.2. Локальное взаимодействие, осуществляемое по каналам .....	147
5.1.3. Обращение через сокеты домена UNIX.....	148
5.1.4. Рассмотрение сокетов netlink .....	149
5.1.5. Действия с сокетами протоколов TCP и UDP .....	150
5.1.6. Вывод списка сетевых соединений с параметрами безопасности....	152
5.2. Межсетевой экран и маркировка сетевых пакетов .....	152
5.2.1. Вводные сведения о межсетевом экране netfilter.....	153
5.2.2. Реализация маркировки сетевых пакетов и соединений .....	154
5.2.3. Назначение меток пакетам .....	155
5.3. Промаркированные сети .....	157
5.3.1. Резервная маркировка в NetLabel.....	158
5.3.2. Ограничение потоков данных на уровне сетевого интерфейса.....	160
5.3.3. Ограничение потоков данных на уровне элементов сети .....	160
5.3.4. Проверка однорангового потока.....	161
5.3.5. Применение управления в старом стиле .....	162
5.4. Метки безопасности для IPsec .....	163
5.4.1. Установка стандартного IPsec .....	165
5.4.2. Подключение маркировки IPsec .....	166
5.4.3. Использование Libreswan .....	167
5.5. Технология маркировки сетей NetLabel с параметром CIPSO.....	168
5.5.1. Настройка сопоставлений потоков данных с доменами .....	169
5.5.2. Добавление сопоставлений для типов допустимого набора функций .....	170
5.5.3. Локальное использование параметра CIPSO .....	171

5.5.4. Поддержка опции безопасности для IPv6 .....	172
5.6. Заключение.....	172

## **Глава 6. Поддержка sVirt и Docker .....**

6.1. Виртуализация, защищенная SELinux .....	173
6.1.1. Представление о виртуализации .....	173
6.1.2. Обзор рисков виртуализации.....	175
6.1.3. Использование типов для объектов виртуальной инфраструктуры .....	176
6.1.4. Перенастраиваемое применение существующих типов виртуализации.....	177
6.1.5. Рассмотрение защиты различных категорий .....	179
6.2. Поддержка библиотеки libvirt .....	180
6.2.1. Различные случаи маркировки ресурсов .....	181
6.2.2. Оценка архитектуры libvirt .....	181
6.2.3. Настройка libvirt для работы с sVirt.....	182
6.2.4. Использование статических параметров безопасности .....	184
6.2.5. Гибкая настройка параметров безопасности.....	184
6.2.6. Использование разных мест хранения.....	185
6.2.7. Интерпретация информации в поле вывода данных о метке .....	185
6.2.8. Управление доступными категориями.....	186
6.2.9. Поддержка интерпретирующих доменов .....	186
6.2.10. Изменение параметров безопасности, установленных по умолчанию .....	187
6.3. Защищенные контейнеры Docker.....	188
6.3.1. Представление о защите контейнера .....	188
6.3.2. Интеграция системы защиты с контейнерами без sVirt.....	189
6.3.3. Перестраховка безопасности Docker средствами защиты sVirt .....	190
6.3.4. Ограничение привилегий контейнера .....	191
6.3.5. Применение различных параметров безопасности для контейнеров .....	193
6.3.6. Перемаркировка подключенного тома данных.....	194
6.3.7. Понижение контроля со стороны SELinux для специальных контейнеров.....	195
6.3.8. Изменение параметров безопасности, установленных по умолчанию .....	195
6.4. Заключение.....	196

## **Глава 7. D-Bus и systemd .....**

7.1. Фоновый процесс системы (systemd).....	197
7.2. Способ поддержки в systemd служб .....	198
7.2.1. Введение понятия модульных файлов.....	198

7.2.2. Установка параметров безопасности SELinux для какой-либо службы .....	199
7.2.3. Использование переходных служб .....	200
7.2.4. Требование включения или отключения SELinux для конкретной службы .....	201
7.2.5. Перемаркировка файлов во время запуска службы .....	202
7.2.6. Использование активизации, основанной на сокетах .....	204
7.2.7. Управление доступом к операциям с модулями .....	205
7.3. Регистрация событий с помощью systemd .....	206
7.3.1. Получение информации, относящейся к SELinux .....	206
7.3.2. Запрос событий, содержащих параметры безопасности SELinux .....	207
7.3.3. Интеграция диагностики неисправностей с журналом .....	207
7.4. Использование контейнеров systemd .....	209
7.4.1. Инициализация контейнеров systemd .....	209
7.4.2. Использование специальных параметров безопасности SELinux .....	209
7.5. Управление файлами устройств .....	210
7.5.1. Использование правил udev .....	210
7.5.2. Назначение метки SELinux на узле устройства .....	212
7.6. Взаимодействие с шиной сообщений D-Bus .....	212
7.6.1. Представление о взаимодействии между процессами D-Bus .....	212
7.6.2. Контроль получения доступа к службам с помощью SELinux .....	215
7.6.3. Управление потоками сообщений .....	216
7.7. Заключение .....	217
<b>Работа с политиками SELinux .....</b>	<b>218</b>
8.1. Логические параметры SELinux .....	218
8.1.1. Вывод списка логических параметров .....	219
8.1.2. Изменение значений логических параметров .....	220
8.1.3. Проверка влияния логического параметра .....	221
8.2. Усиление политик SELinux .....	222
8.2.1. Список модулей политики .....	222
8.2.2. Загрузка и удаление модулей политики .....	223
8.2.3. Создание политик с использованием программы audit2allow .....	224
8.2.4. Использование говорящих за себя наименований для модулей политики .....	226
8.2.5. Использование макрокоманд посреднической политики с программой audit2allow .....	227
8.2.6. Использование скрипта selocal .....	228
8.3. Создание модулей политик по специальным требованиям .....	229
8.3.1. Создание модулей SELinux с помощью исходного языка описания политик .....	230
8.3.2. Создание модулей SELinux с помощью посреднического стиля описания политик .....	231

8.3.3. Создание модулей SELinux с помощью обобщенно-промежуточного языка.....	232
8.3.4. Добавление описаний для параметров безопасности файла .....	232
8.4. Создание ролей и пользовательских типов допустимого набора функций .....	233
8.4.1. Создание файла <code>pgsql_admin.te</code> .....	233
8.4.2. Создание прав пользователя.....	234
8.4.3. Предоставление доступа для взаимодействия с командным интерфейсом.....	235
8.4.4. Формирование структуры файлов пользовательской политики.....	236
8.5. Создание новых типов для приложений.....	237
8.5.1. Создание файлов <code>mojomojo.*</code> .....	238
8.5.2. Создание интерфейсов политик .....	239
8.5.3. Создание структуры файлов политики для приложений.....	240
8.6. Замена существующих политик.....	241
8.6.1. Замена политик Red Hat Enterprise Linux .....	241
8.6.2. Замена политик в Gentoo .....	243
8.7. Другие варианты усиления политики безопасности.....	244
8.7.1. Создание типов SECMARK по специальным требованиям .....	244
8.7.2. Регистрация попыток доступа в журнале событий.....	245
8.7.3. Создание типов, соответствующих специальным требованиям .....	245
8.8. Заключение.....	246

## **Глава 9. Анализ поведения политики .....**

9.1. Одноступенчатый анализ.....	248
9.1.1. Использование различных файлов политик SELinux.....	249
9.1.2. Отображение информации об объектах политики .....	249
9.1.3. Применение утилиты <code>sesearch</code> .....	251
9.1.4. Запрос разрешающих правил .....	251
9.1.5. Запрос сведений о правилах преобразования типов .....	251
9.1.6. Запрос правил для других типов.....	252
9.1.7. Запрос правил, связанных с ролями .....	253
9.1.8. Отображение данных с помощью графической программы <code>apol</code> .....	253
9.2. Анализ преобразований типов процессов .....	257
9.2.1. Использование программы <code>apol</code> .....	258
9.2.2. Использование программы <code>sedta</code> .....	259
9.3. Анализ потоков информации .....	261
9.3.1. Использование программы <code>apol</code> для анализа потоков информации .....	262
9.3.2. Использование программы <code>seinfoflow</code> для анализа потоков информации .....	265
9.4. Другие виды анализа политик .....	266
9.4.1. Сравнение политик при помощи <code>sediff</code> .....	266



9.4.2. Анализ политик при помощи sepolisy .....	267
9.5. Заключение.....	268

## **Глава 10. Частные случаи настройки защиты..... 269**

10.1. Усиление защиты веб-серверов .....	269
10.1.1. Описание условий работы .....	270
10.1.2. Настройка для установки нескольких экземпляров программ .....	271
10.1.3. Создание категорий SELinux .....	272
10.1.4. Выбор необходимых параметров безопасности.....	273
10.1.5. Включение администраторов в систему защиты .....	275
10.1.6. Управление работой веб-сервера.....	275
10.1.7. Работа с обновлением содержания .....	277
10.1.8. Настройка сети и правил межсетевого экрана.....	279
10.2. Защита командно-строчного интерфейса .....	279
10.2.1. Разделение SSH на несколько экземпляров .....	280
10.2.2. Обновление правил работы сети .....	281
10.2.3. Изменение корневого каталога для отдельной программы .....	282
10.2.4. Предоставление параметров безопасности пользователю в зависимости от способа доступа .....	283
10.2.5. Настройка правил для SSH .....	285
10.2.6. Включение многопользовательского режима использования .....	286
10.3. Общий доступ к файлам через сетевую файловую систему NFS .....	287
10.3.1. Базовая настройка службы NFS .....	287
10.3.2. Включение поддержки NFS на стороне защищенного клиента .....	288
10.3.3. Настройка правил безопасности для NFS на сервере .....	288
10.3.4. Подключение общих сетевых ресурсов с различными параметрами безопасности .....	289
10.3.5. Работа с промаркированной сетевой файловой системой .....	290
10.3.6. Сравнение файлового сервера Samba с сетевой файловой системой NFS .....	291
10.4. Заключение.....	292

## **Предметный указатель..... 293**