Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Кондрашина Мария Сергеевна

Содержание

# 1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1.

Проверить работу SELinx на практике совместно с веб-сервером Apache.

# 2 Теоретические сведения

SELinux (англ. Security-Enhanced Linux — Linux с улучшенной безопасностью) — реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа.[2]

# 3 Выполнение лабораторной работы. Создание программы

1. Подготовка лабораторного стенда (fig. 1) -

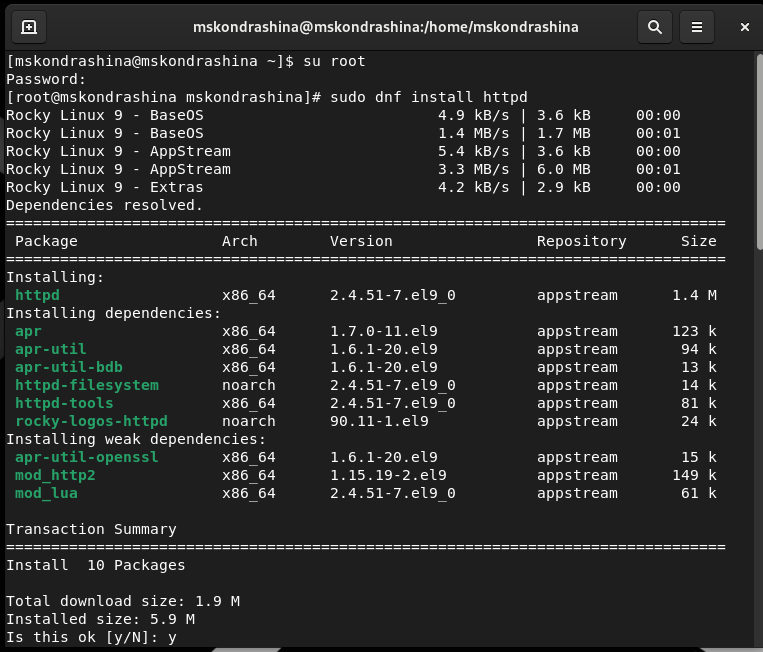


Figure 1: Подготовка лабораторного стенда

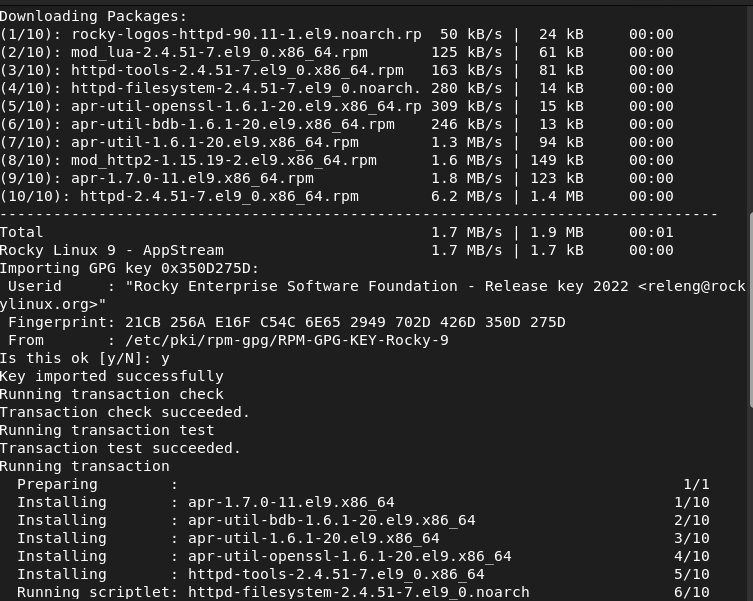


Figure 2: Подготовка лабораторного стенда

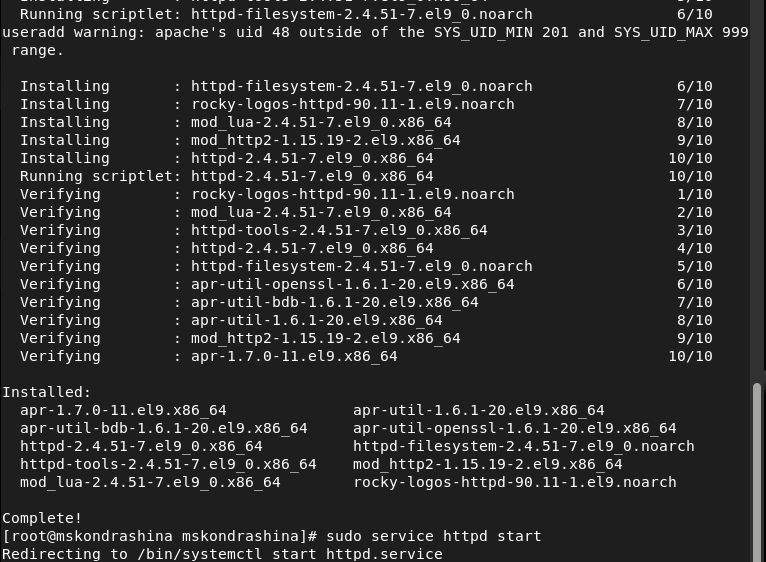


Figure 3: Подготовка лабораторного стенда

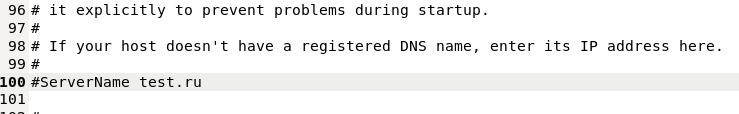


Figure 4: Подготовка лабораторного стенда

Figure 5: Подготовка лабораторного стенда

Figure 5: Подготовка лабораторного стенда

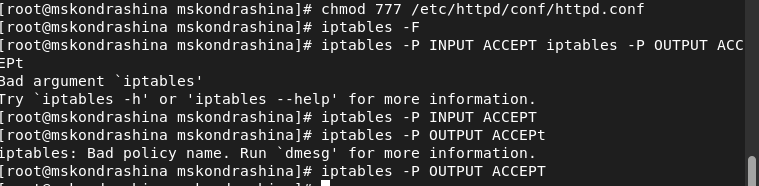


Figure 6: Подготовка лабораторного стенда

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus(fig. 7)

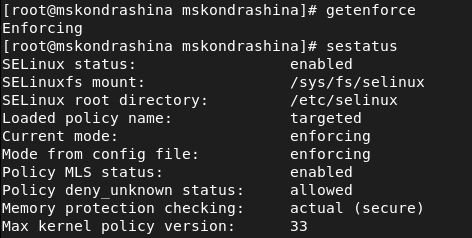


Figure 7: getenforce и sestatus

1. Обратилась с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедилась, что последний работает: (fig. 8)

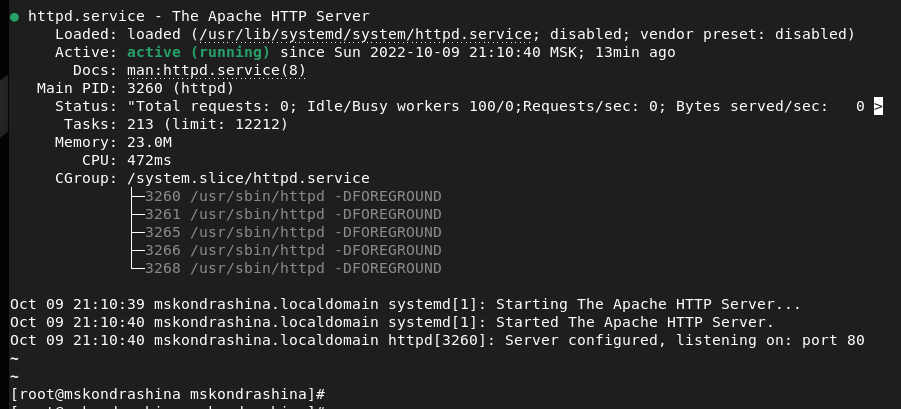


Figure 8: Обратилась с помощью браузера к веб-серверу, запущенному на компьютере

1. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности и занесла эту информацию в отчёт (httpd\_t). (fig. 9)

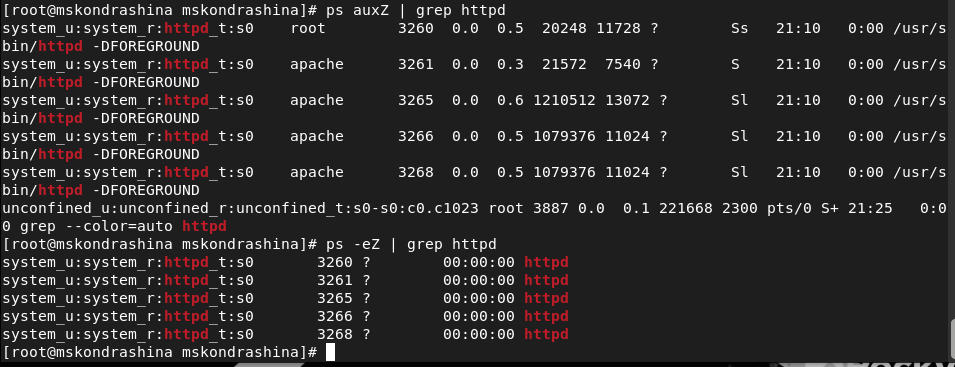


Figure 9: Веб-сервер Apache в списке процессов, его контекст безопасности

1. Посмотрела текущее состояние переключателей SELinux для Apache. (fig. 10)

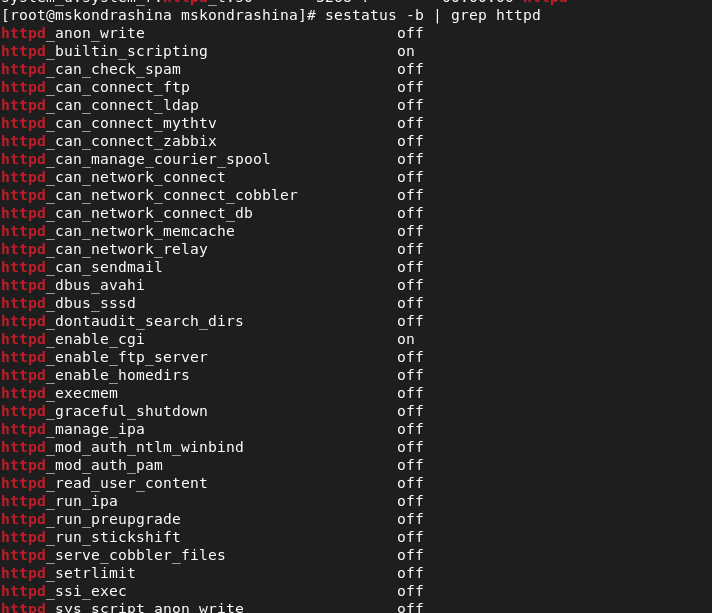


Figure 10: Текущее состояние переключателей SELinux для Apache

1. Посмотрела статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов. (fig. 11)

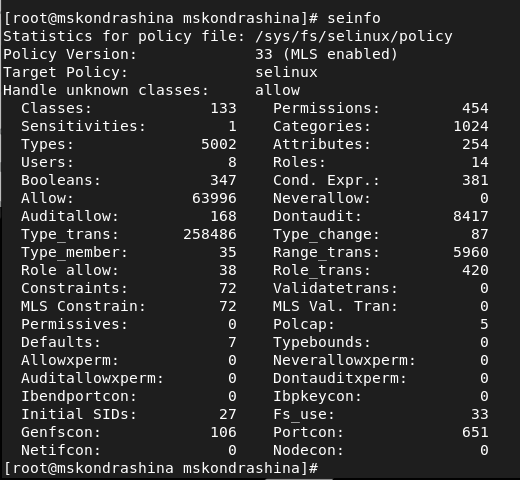


Figure 11: Cтатистика по политике с помощью команды seinfo

* Множество пользователей: 8
* Роли: 14
* Типы: 5002

1. Определила тип файлов и поддиректорий, находящихся в директории /var/www и /var/www/html (fig. 12)

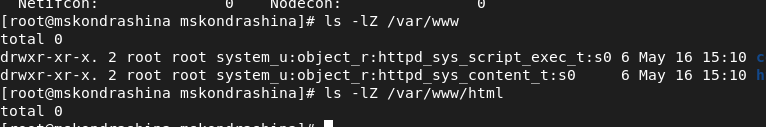


Figure 12: Тип файлов и поддиректорий, находящихся в директории /var/www и /var/www/html

Круг пользователей, которым разрешено создание файлов в директории - пользователь (user)

1. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html (fig. 13) - (fig. 14)

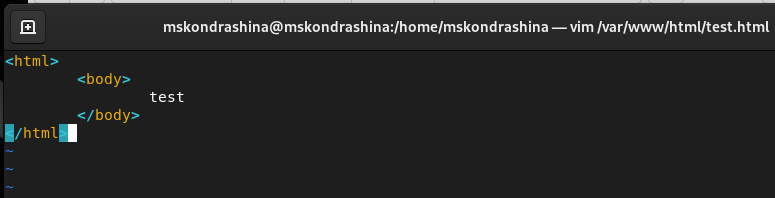


Figure 13: Создайте от имени суперпользователя html-файл /var/www/html/test.html

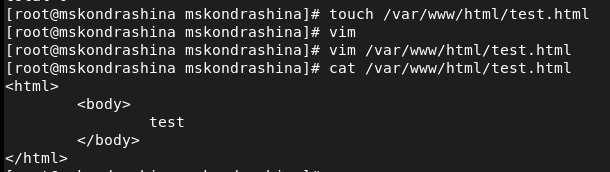


Figure 14: Создайте от имени суперпользователя html-файл /var/www/html/test.html (консоль)

1. Проверила контекст созданного файла. Занесла в отчёт контекст - httpd\_sys\_content\_t, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html (fig. 15)

Figure 15: Контекст созданного файла

Figure 15: Контекст созданного файла

1. Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедилась, что файл был успешно отображён.(fig. 16)

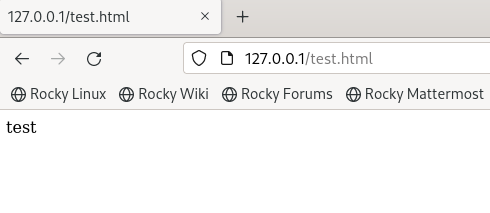


Figure 16: Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html

1. Тип файла test.html - httpd\_sys\_content\_t. Тип httpd\_sys\_content\_t позволяет процессу httpd получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.(fig. 17)

Figure 17: Тип файла test.html

Figure 17: Тип файла test.html

1. Изменила контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t(fig. 18)

Figure 18: Изменила контекст файла test.html с httpd_sys_content_t на samba_share_t

Figure 18: Изменила контекст файла test.html с httpd\_sys\_content\_t на samba\_share\_t

1. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html.(fig. 19)

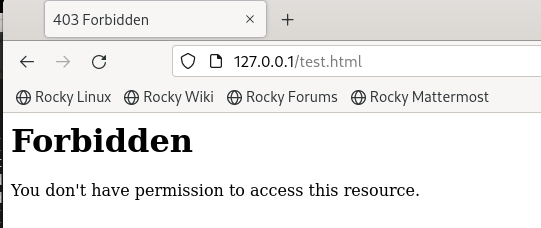


Figure 19: Попробовала ещё раз получить доступ к файлу через веб-сервер

1. Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл(fig. 20)

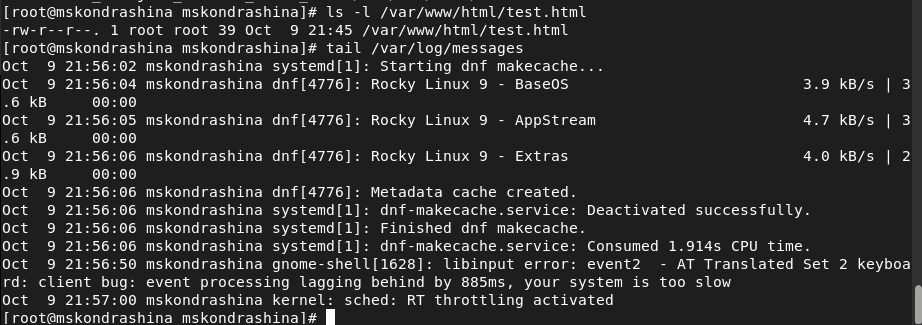


Figure 20: Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл

1. Попробовала запустить веб-сервер Apache на прослушивание ТСР-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81. (fig. 21)

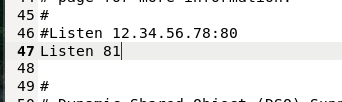


Figure 21: В файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81

1. Выполнила перезапуск веб-сервера Apache. Сбой не произошёл. Проанализирова лог-файлы tail -nl /var/log/messages.(fig. 22)

Просмотрела файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выяснила, в каких файлах появились записи - только в /var/log/audit/audit.log. (fig. 23)

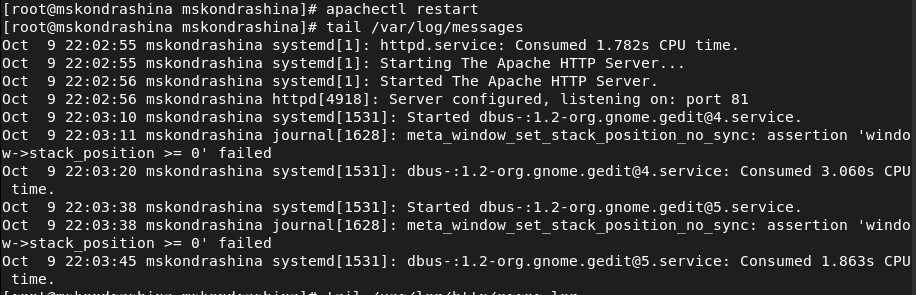


Figure 22: Проанализирова лог-файлы /var/log/messages

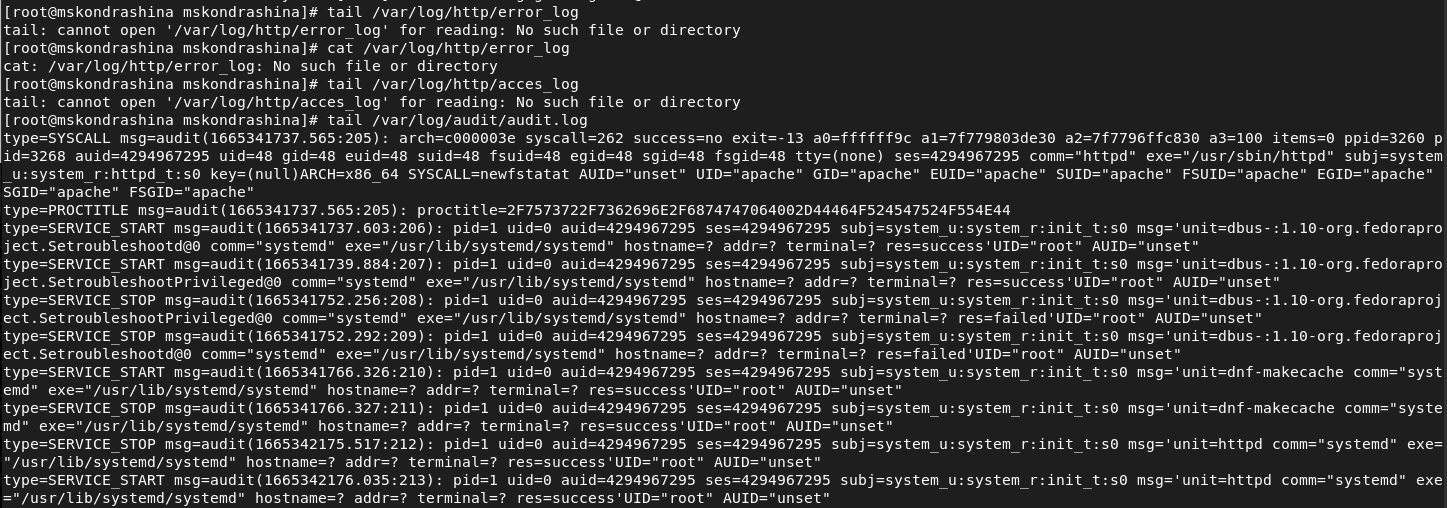


Figure 23: Просмотрела файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log

1. Выполнила команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверила список портов командой semanage port -l | grep http\_port\_t. Убедилась, что порт 81 появился в списке.(fig. 24)

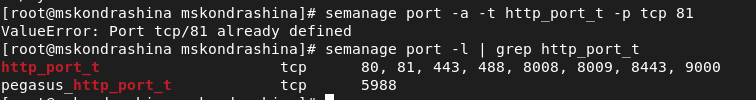


Figure 24: Список портов

1. Попробовала запустить веб-сервер Apache ещё раз, он снова запустился. Вернула контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/test.html. После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. (fig. 25)-(fig. 26)

Figure 25: Запуск веб-сервера Apache ещё раз и возвращение контекста httpd_sys_cоntent__t к файлу test.html

Figure 25: Запуск веб-сервера Apache ещё раз и возвращение контекста httpd\_sys\_cоntent\_\_t к файлу test.html

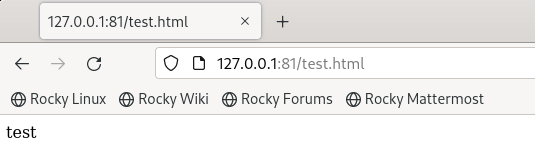


Figure 26: Попытка получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html

1. Исправила обратно конфигурационный файл apache, вернув Listen 80. (fig. 27)

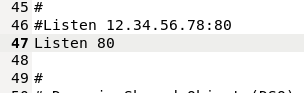


Figure 27: Исправила обратно конфигурационный файл apache, вернув Listen 80

1. Попыталась удалить привязку http\_port\_t к 81 порту, что не получилось так как 81 порт defined in policy и не может быть удален. Удалила файл /var/www/html/test.html (fig. 28)

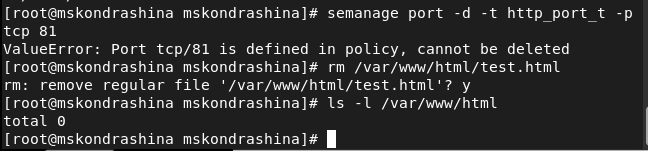


Figure 28: Попытка удалить привязку http\_port\_t к 81 порту и удаление файла test.html

# 4 Выводы

Выполнила лабораторную работу №6.

Развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux1.

Проверила работу SELinx на практике совместно с веб-сервером Apache.

# 5 Список литературы

1. Методические материалы курса. “Информационная безопасность компьютерных сетей” Кулябов Д. С., Королькова А. В., Геворкян М. Н.
2. https://ru.wikipedia.org/wiki/SELinux