Отчёт по лабораторной работе №6. Мандатное разграничение прав в Linux

Предмет: информационная безопасность

Александр Сергеевич Баклашов

Содержание

# 1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache. [1]

# 2 Теоретическое введение

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

# 3 Выполнение лабораторной работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus. (рис. [1](#fig:001))

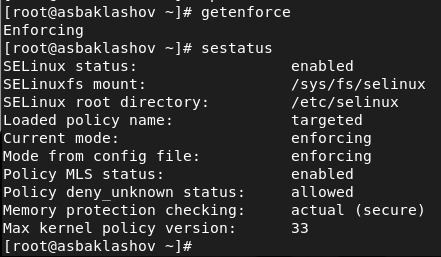


Figure 1: getenforce и sestatus

1. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает (рис. [2](#fig:002))

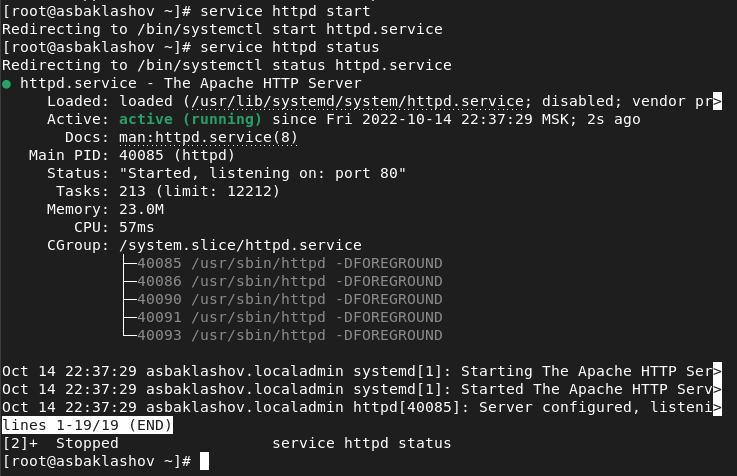


Figure 2: Веб-сервер

1. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. (рис. [3](#fig:003))

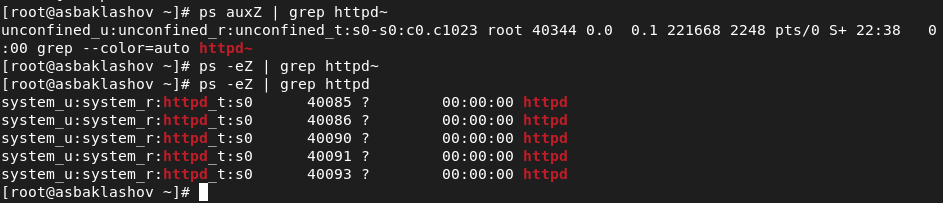


Figure 3: Apache

httpd\_sys\_cоntent\_t

1. Посмотрите текущее состояние переключателей SELinux для Apache. (рис. [4](#fig:004))

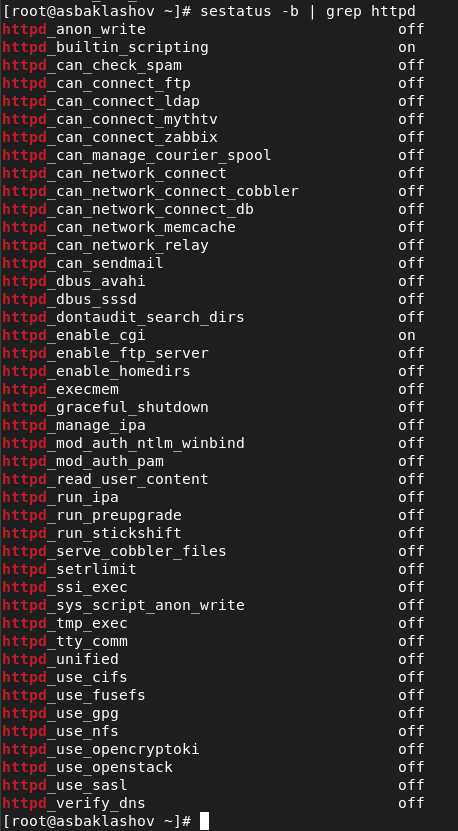


Figure 4: Cостояние переключателей

1. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов. (рис. [5](#fig:005))

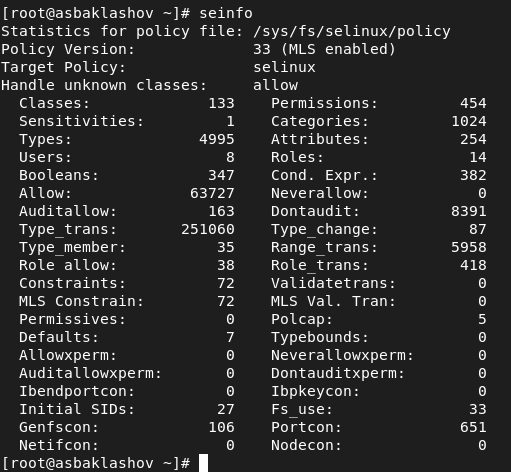


Figure 5: seinfo

1. Определите тип файлов и поддиректорий, находящихся в директории /var/www (рис. [6](#fig:006))

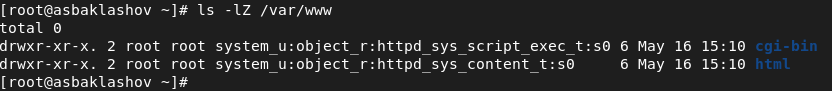


Figure 6: тип

1. Определите тип файлов, находящихся в директории /var/www/html (рис. [7](#fig:007))

Figure 7: тип

Figure 7: тип

1. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html (рис. [8](#fig:008))

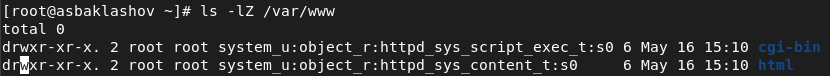


Figure 8: круг пользователей

Только владелец

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

< html >

< body >test< /body >

< /html >

(рис. [9](#fig:009))

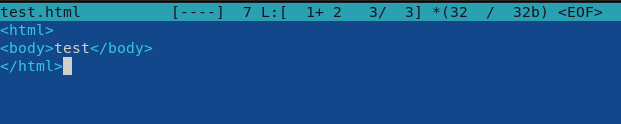


Figure 9: файл

1. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html (рис. [10](#fig:010))

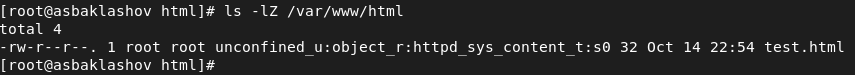


Figure 10: контекст

httpd\_sys\_cоntent\_t

1. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён. (рис. [11](#fig:011))

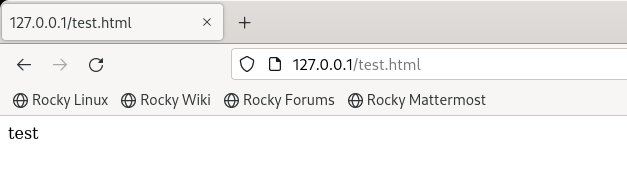


Figure 11: http://127.0.0.1/test.html

Файл был успешно отображён

1. Проверить контекст файла /var/www/html/test.html командой ls -Z. ls -Z /var/www/html/test.html (рис. [12](#fig:012))

Figure 12: Проверка

Figure 12: Проверка

1. Измените контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba\_share\_t (рис. [13](#fig:013))

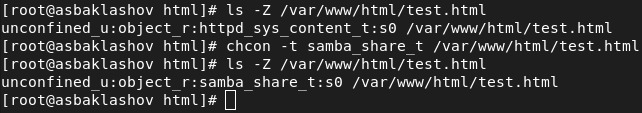


Figure 13: Смена контекста

1. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Вы должны получить сообщение об ошибке (рис. [14](#fig:014))

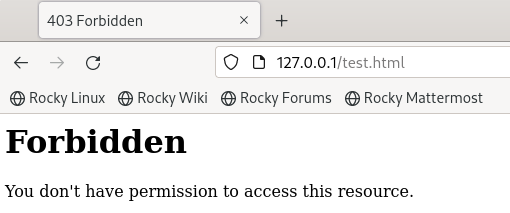


Figure 14: Ошибка

1. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю?

Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: tail /var/log/messages (рис. [15](#fig:015))



Figure 15: log-файлы

1. Попробуйте 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 найдите строчку Listen 80 и замените её на Listen 81. (рис. [16](#fig:016))

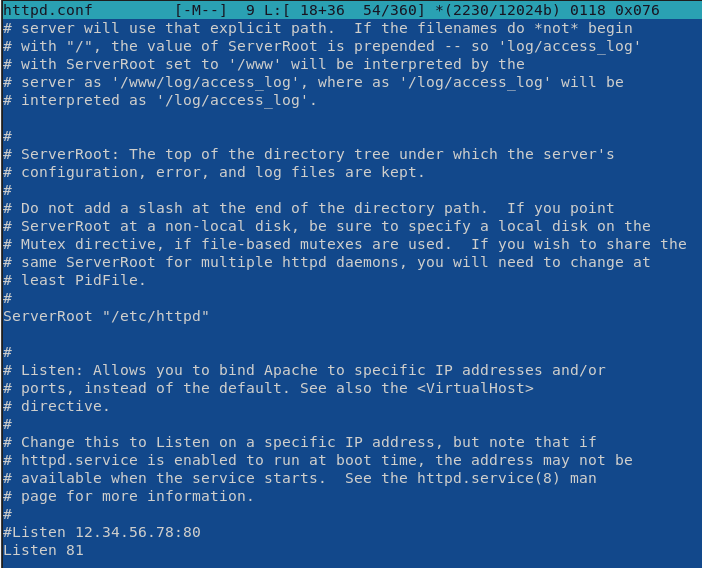


Figure 16: Замена

1. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?

Сбоя нет.

1. Проанализируйте лог-файлы: tail -nl /var/log/messages Просмотрите файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выясните, в каких файлах появились записи. (рис. [17](#fig:0181), рис. [18](#fig:0182),рис. [19](#fig:0183))

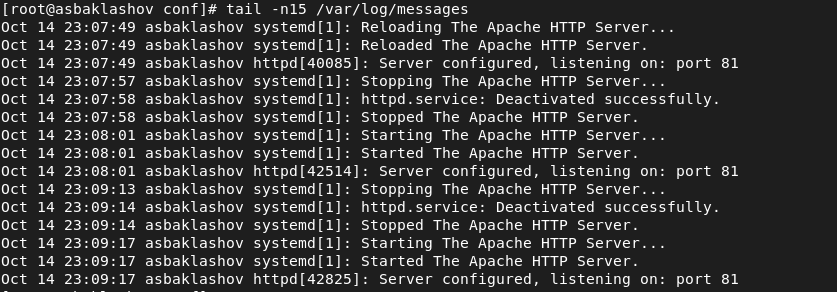


Figure 17: /var/log/messages



Figure 18: /var/log/http/access\_log

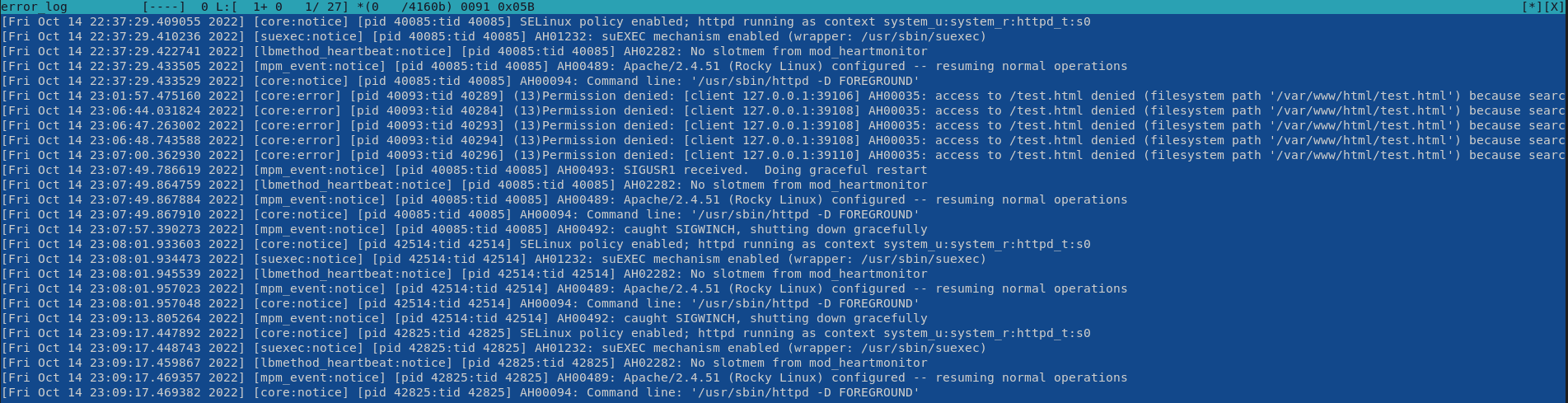


Figure 19: /var/log/http/error\_log

1. Выполните команду semanage port -a -t http\_port\_t -р tcp 81

После этого проверьте список портов командой semanage port -l | grep http\_port\_t Убедитесь, что порт 81 появился в списке. (рис. [20](#fig:019))

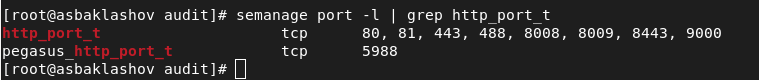


Figure 20: 81

Порт 81 был в списке до этого, поэтому сбоя не было.

1. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог?

Сервер запускался и до этого. Он бы не запустился, если бы порта 81 изначально не было в списке.

1. Верните контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html: chcon -t httpd\_sys\_content\_t /var/www/html/test.html После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Вы должны увидеть содержимое файла — слово «test». (рис. [21](#fig:025), рис. [22](#fig:021))

Figure 21: «test»

Figure 21: «test»

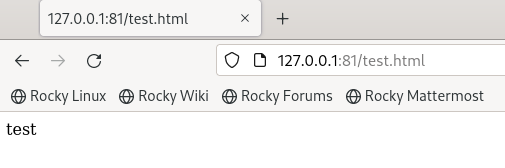


Figure 22: «test»

1. Исправьте обратно конфигурационный файл apache, вернув Listen 80. (рис. [23](#fig:022))

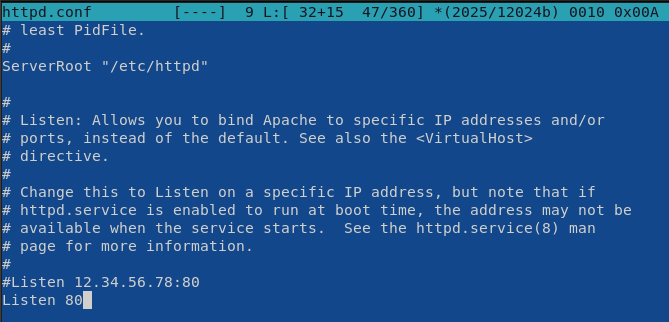


Figure 23: Listen 80

1. Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 (рис. [24](#fig:023))

Figure 24: 81

Figure 24: 81

Не вышло

1. Удалите файл /var/www/html/test.html (рис. [25](#fig:024))

Figure 25: Удалите файл

Figure 25: Удалите файл

# 4 Вывод

В результате выполнения работы я развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.

# 5 Библиография

1. Лабораторная работа № 6. Мандатное разграничение прав в Linux. - 5 с. [Электронный ресурс]. М. URL: [Лабораторная работа №6](https://esystem.rudn.ru/pluginfile.php/1651891/mod_resource/content/2/006-lab_selinux.pdf) (Дата обращения: 15.10.2022).
2. Rocky Linux Documentation. [Электронный ресурс]. М. URL: [Rocky Linux Documentation](https://docs.rockylinux.org) (Дата обращения: 15.10.2022).