Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Смородова Дарья Владимировна

2022 Oct 15th

Содержание

# Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Теоретическое введение[[1]](#footnote-21)

Apache HTTP-сервер (является искажённым сокращением от англ. a patchy server; среди русских пользователей общепринято переводное апа́ч) — свободный веб-сервер.

Apache является кроссплатформенным ПО, поддерживает операционные системы Linux, BSD, macOS, Microsoft Windows, Novell NetWare, BeOS.

Основными достоинствами Apache считаются надёжность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и т. д. Поддерживает IPv4.

Сервер был написан в начале 1995 года и считается, что его имя восходит к шуточному названию «a patchy» (с англ. — «в заплатках»), так как он устранял ошибки популярного тогда сервера Всемирной паутины NCSA HTTPd 1.3. В дальнейшем, с версии 2.х, сервер был переписан заново и теперь не содержит кода NCSA. На данный момент разработка ведётся в ветке 2.4, а в версиях 1.3, 2.0 и 2.2 производятся лишь исправления ошибок безопасности. На текущий момент последняя версия ветки 2.4 — 2.4.46 (5 августа 2020), для первой версии это 1.3.42.

Веб-сервер Apache разрабатывается и поддерживается открытым сообществом разработчиков под эгидой Apache Software Foundation и включён во многие программные продукты, среди которых СУБД Oracle и IBM WebSphere.

# Выполнение лабораторной работы[[2]](#footnote-23)

1. В конфигурационном файле /etc/httpd/httpd.conf зададим параметр ServerName (рис. 1):

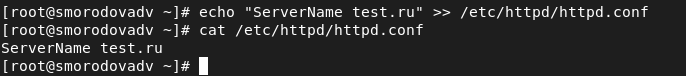


Figure 1: Задание параметра ServerName

1. Также проследим, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключим фильтр и добавим разрешающие правила (рис. 2):

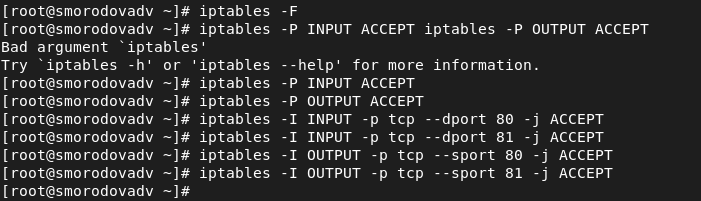


Figure 2: Отключение фильтра

1. Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted (рис. 3):

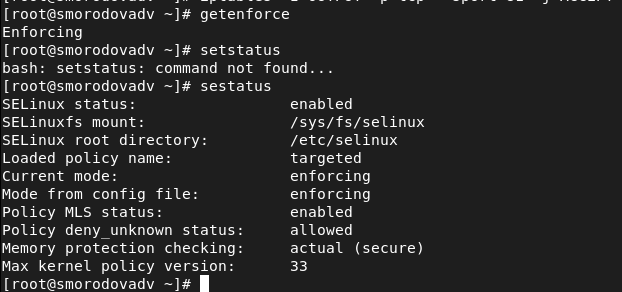


Figure 3: Проверка режима и политики

1. Обратимся с помощью браузера к веб-серверу, запущенному на компьютере, и убедимся, что последний работает (рис. 4):

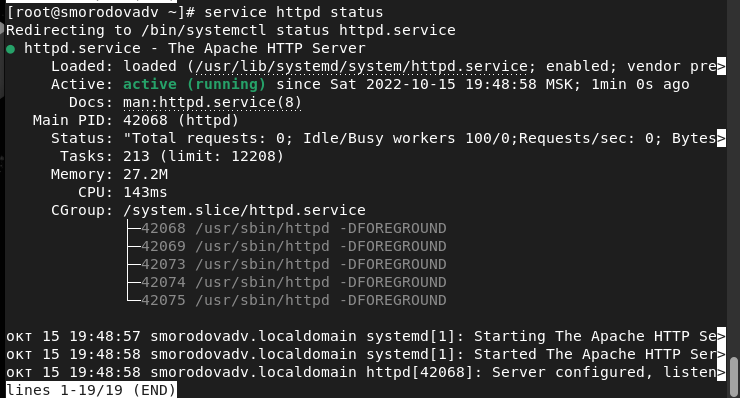


Figure 4: Проверка статуса

1. Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности (рис. 5):

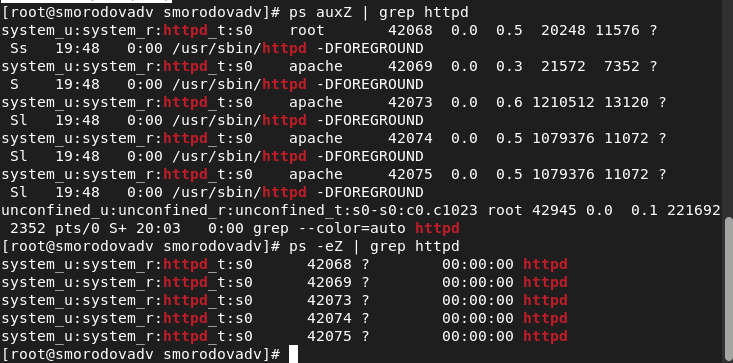


Figure 5: Веб-сервер Apache

1. Посмотрим текущее состояние переключателей SELinux для Apache (рис. 6):

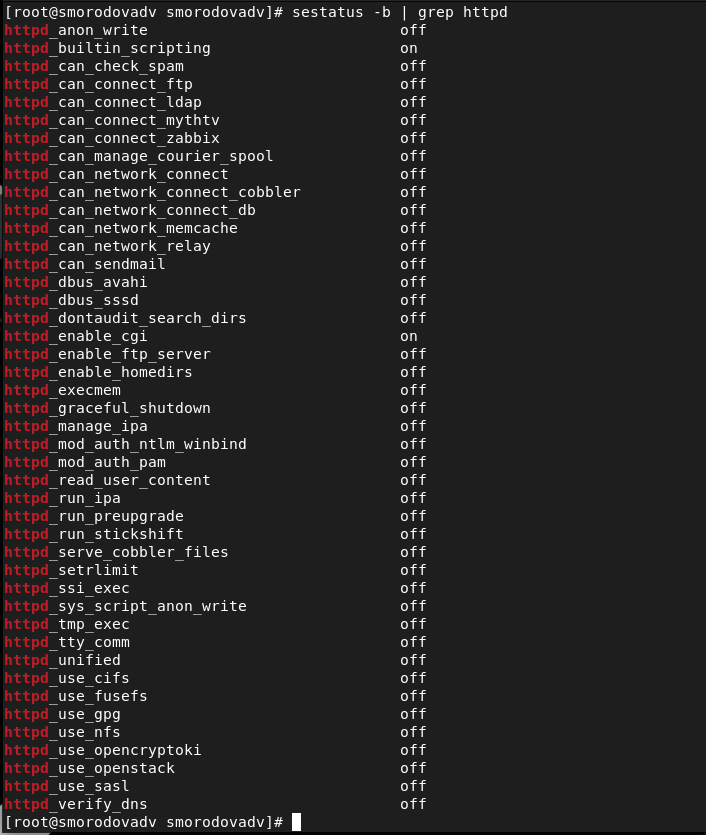


Figure 6: Просмотр переключателей SELinux для Apache

1. Посмотрим статистику по политике, а также определим множество пользователей(8), ролей(14), типов(5002). (рис. 7):



Figure 7: Статистика по политике

1. Определим тип файлов и поддиректорий, находящихся в директории /var/www (рис. 8):

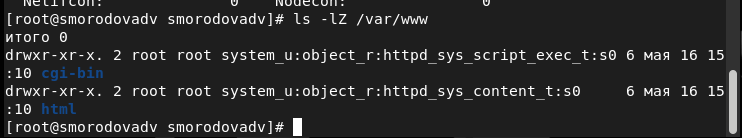


Figure 8: Определение типов файлов и поддиректорий в директории /var/www

1. Определим тип файлов, находящихся в директории /var/www/html и круг пользователей, которым разрешено создание файлов в директории /var/www/html (рис. 9):

Figure 9: Определение типов файлов в директории /var/www/html

Figure 9: Определение типов файлов в директории /var/www/html

1. Создадим от имени суперпользователя html-файл /var/www/html/test.html (рис. 10):

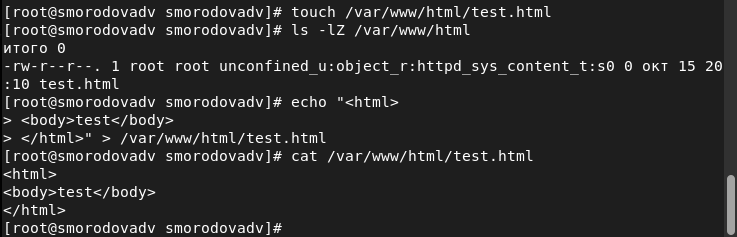


Figure 10: Создание файла

1. Проверим контекст созданного файла: httpd\_sys\_content\_t (рис. 11):

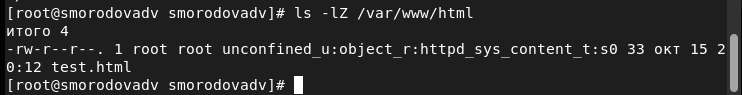


Figure 11: Проверка контекста

1. Обратимся к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедимся, что файл был успешно отображён (рис. 12):

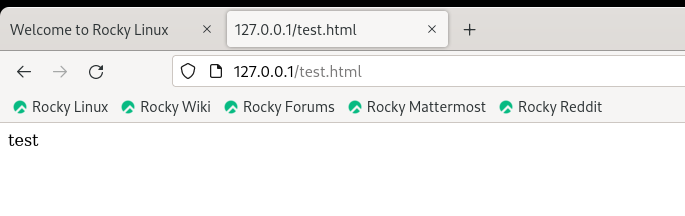


Figure 12: Получение доступа к файлу через браузер

1. Проверим контекст файла (рис. 13):

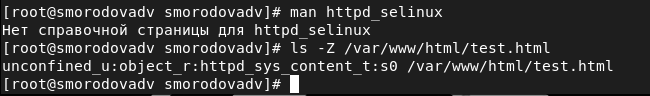


Figure 13: Проверка контекста файла

1. Изменим контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t. После этого проверим, что контекст поменялся (рис. 14):

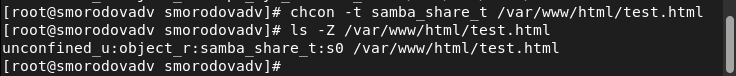


Figure 14: Изменение контекста файла /var/www/html/test.html

1. Попробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получим сообщение об ошибке, так как мы ранее изменили контекст файла(рис. 15):

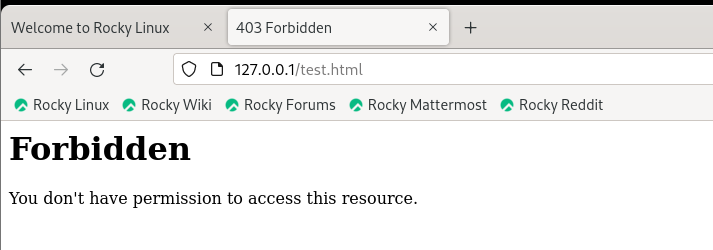


Figure 15: Получение доступа к файлу через браузер

1. Просмотрим log-файлы веб-сервера Apache. Также просмотрем системный лог-файл (рис. 16):

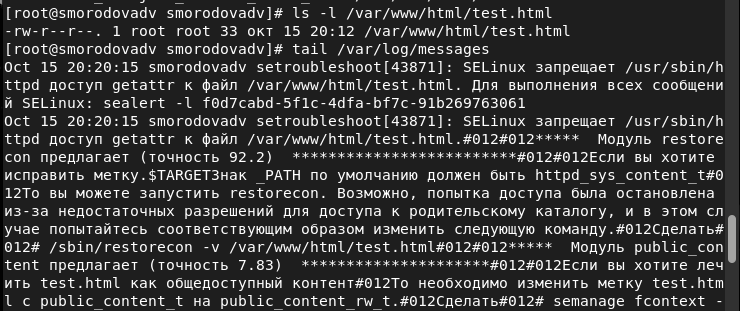


Figure 16: Просмотр log-файла веб-сервера Apache

1. Попробуем 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 найдем строчку Listen 80 и заменим её на Listen 81 (рис. 17):

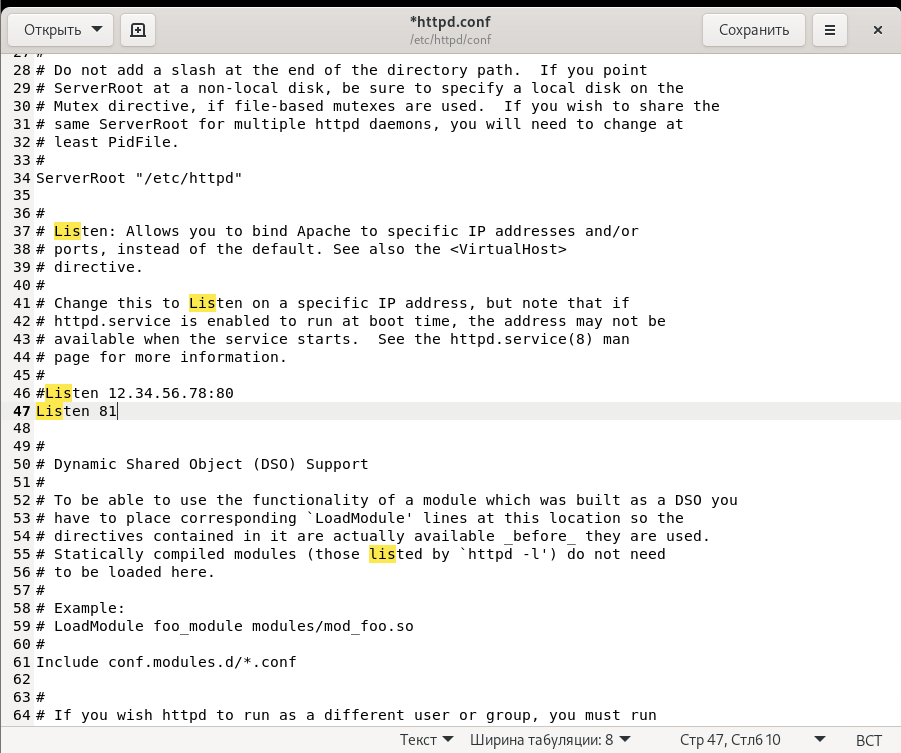


Figure 17: Изменеие ТСР-порта с 80 на 81

1. Просмотрим файлы /var/log/http/error\_log /var/log/http/access\_log и /var/log/audit/audit.log (рис. 18):

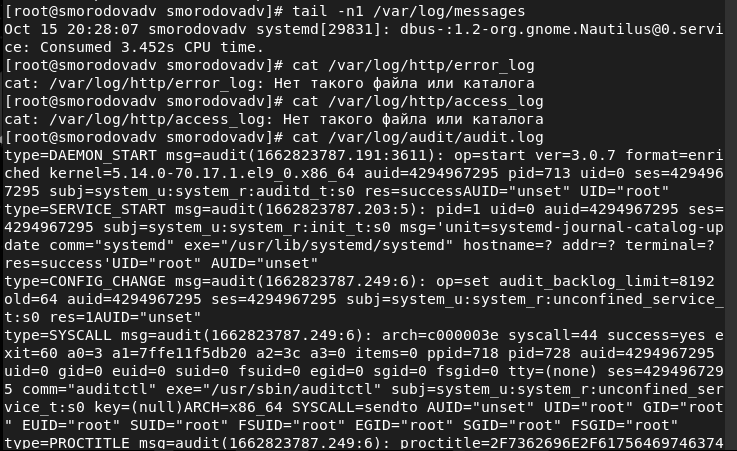


Figure 18: Анализ и просмотр лог-файлов

1. Выполним команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверим список портов. Убедимся, что порт 81 появился в списке (рис. 19):

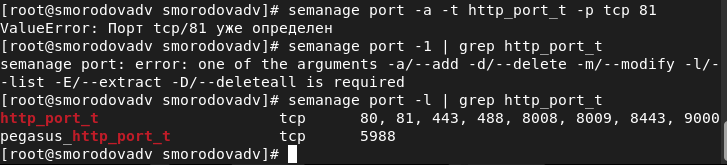


Figure 19: Выполнение и проверка списка портов

1. Вернем контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/test.html (рис. 20):

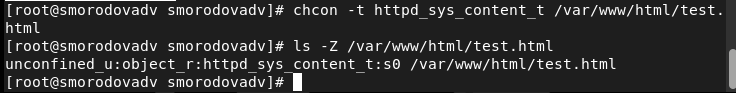


Figure 20: Возвращение контекста

1. Попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Снова увидим содержимое файла — слово «test» (рис. 21):

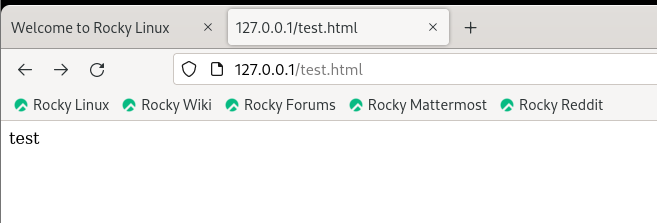


Figure 21: Получение доступа к файлу через браузер

1. Исправим обратно конфигурационный файл apache, вернув Listen80 (рис. 22):

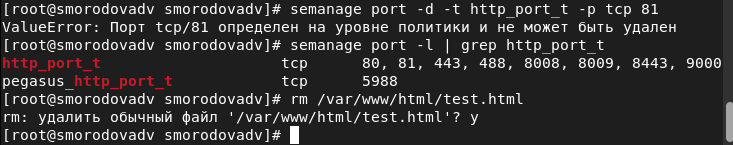


Figure 22: Исправленный файл apache

1. Удалим привязку http\_port\_t к 81 порту и удалим файл /var/www/html/test.html (рис. 23):

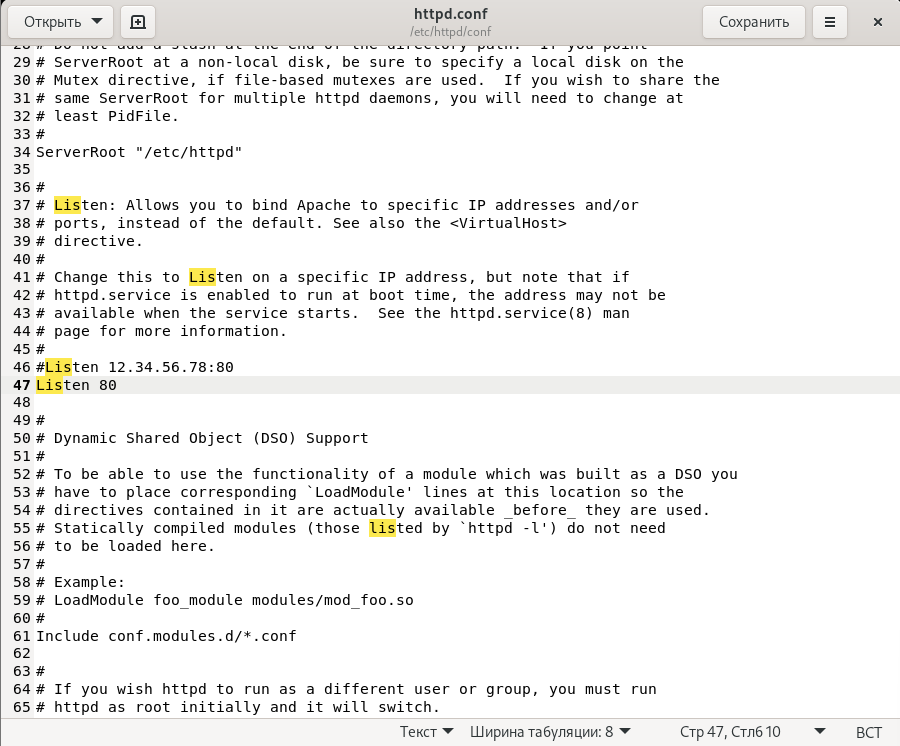


Figure 23: Удаление привязки к 81 порту и удаление файла

# Выводы

В ходе выполнения данной лабораторной работы, мы развили навыки администрирования ОС Linux, получили первое практическое знакомство с технологией SELinux и проверили работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. [Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН”](https://esystem.rudn.ru/)
2. [Wikipedia. Apache HTTP Server](https://ru.wikipedia.org/wiki/Apache_HTTP_Server)

1. Wikipedia. Apache HTTP Server [↑](#footnote-ref-21)
2. Методические материалы к лабораторной работе [↑](#footnote-ref-23)