Отчет по лабораторной работе №6

Основы информационной безопасности

Ищенко Ирина НПИбд-02-22

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus. Обратимся с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедимся, что последний работает (рис. 1) и (рис. 2): service httpd status

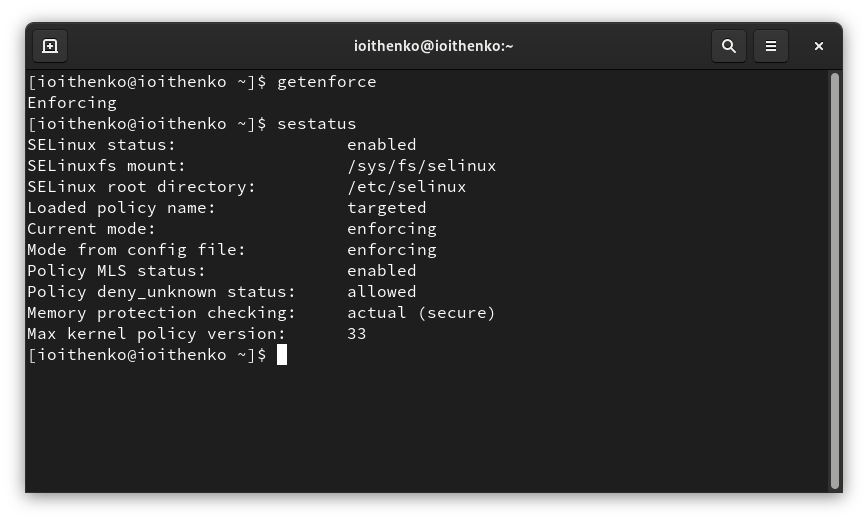


Рис. 1: Проверка статуса

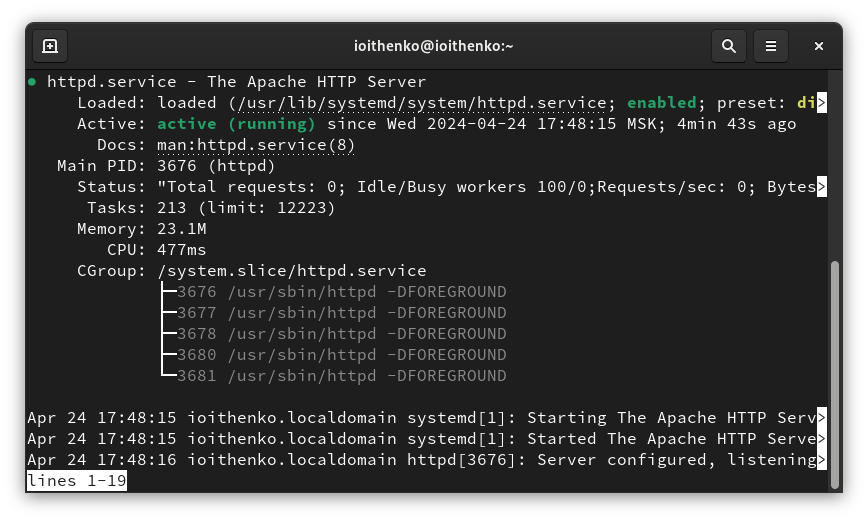


Рис. 2: Проверка статуса

Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности ps auxZ | grep httpd

Посмотрим текущее состояние переключателей SELinux для Apache с помощью команды (рис. 3). sestatus -b | grep httpd

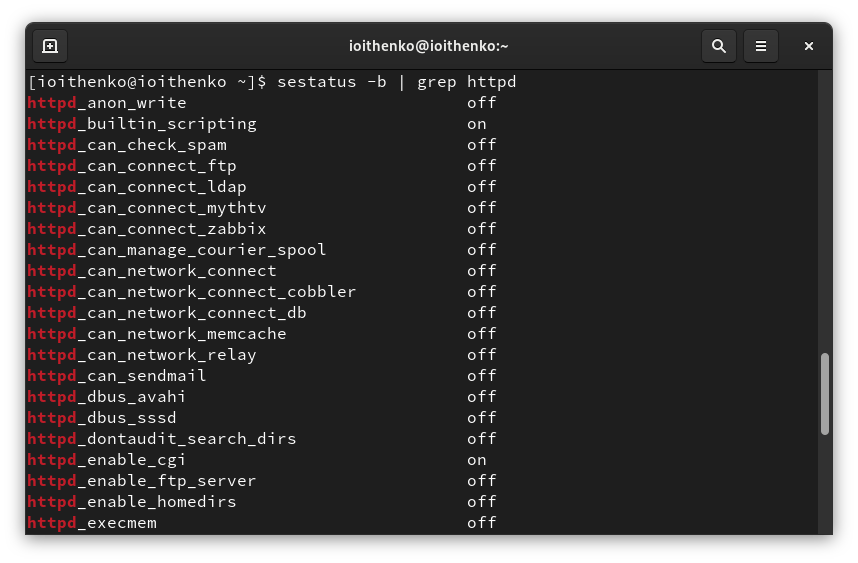


Рис. 3: Переключатели

Посмотрим статистику по политике с помощью команды seinfo, также определим множество пользователей, ролей, типов (рис. 4).

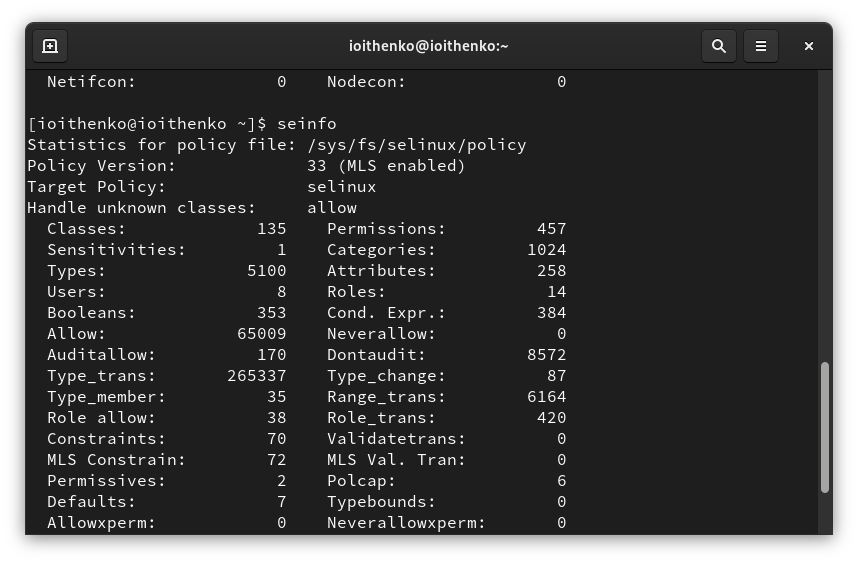


Рис. 4: Статистика по политике

Определим тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды (рис. 5). ls -lZ /var/www

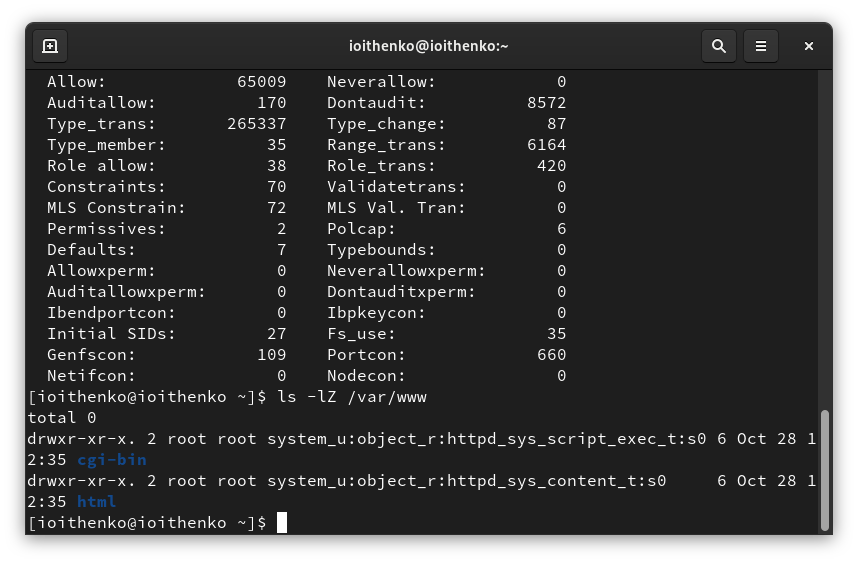


Рис. 5: Типы файлов и поддиректории

Определим тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html. Создадим от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания (рис. 6):

test

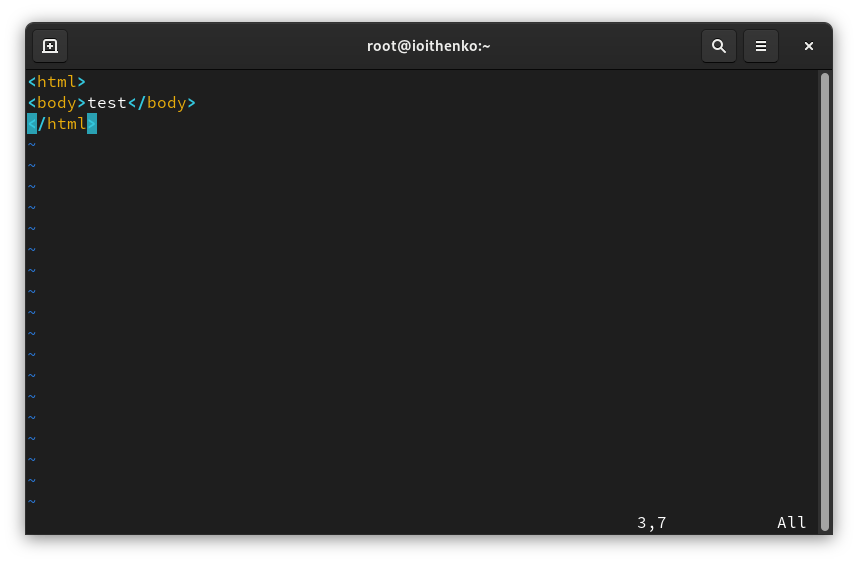


Рис. 6: Файл

Проверим контекст созданного вами файла (рис. 7).

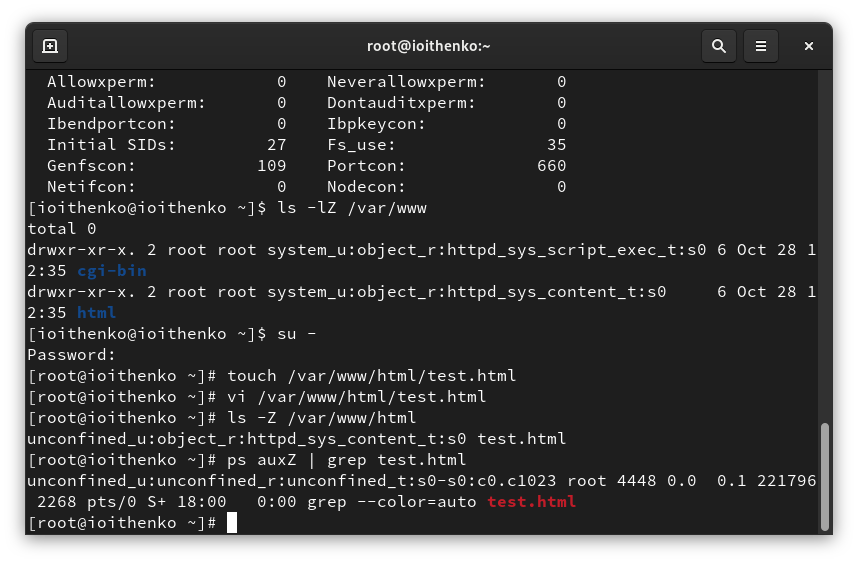


Рис. 7: Контекст

Обратимся к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедимся, что файл был успешно отображён (рис. 8).

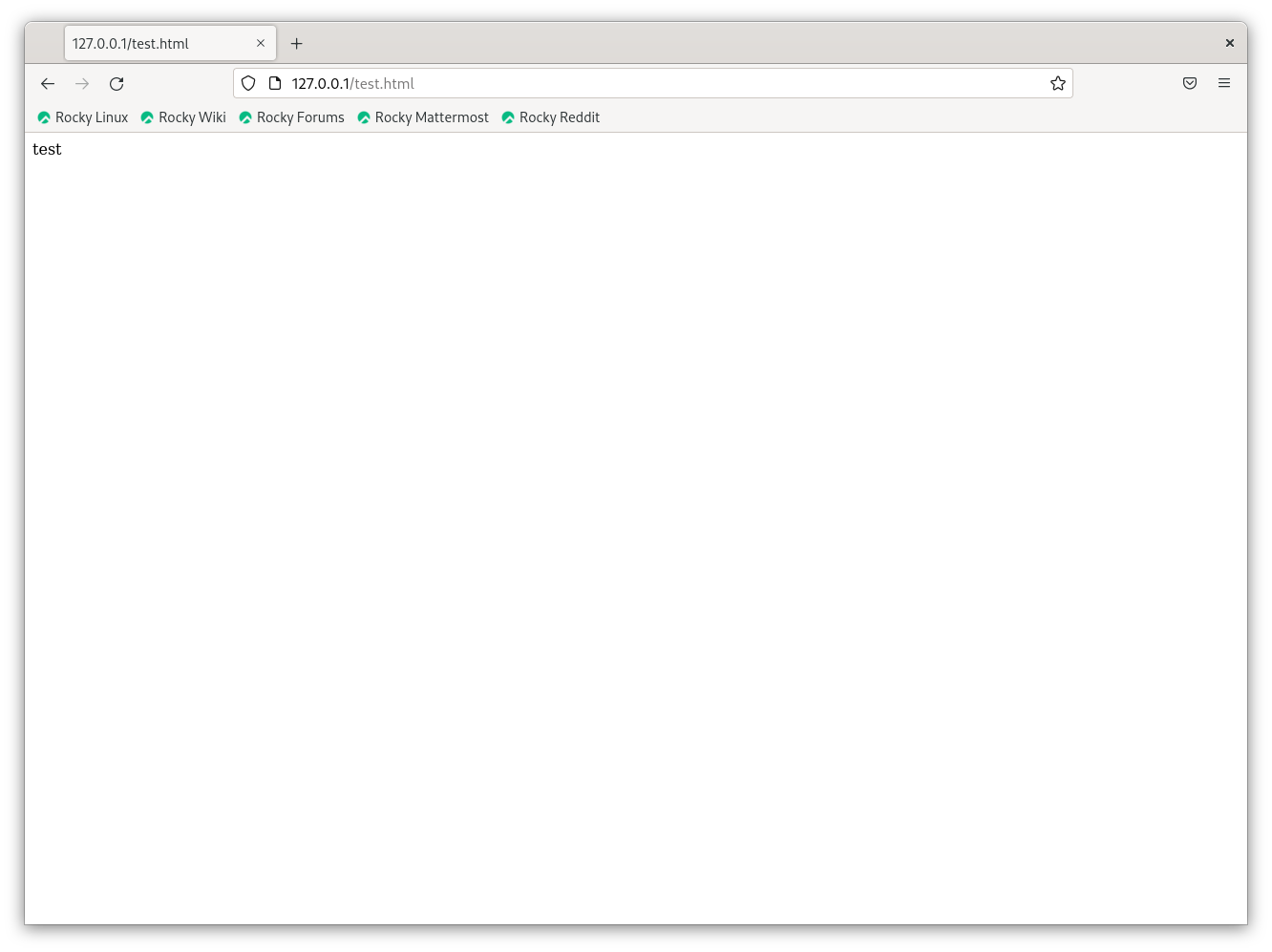


Рис. 8: Проверка отображения файла

Изучим справку man httpd\_selinux и выясним, какие контексты файлов определены для httpd. Сопоставим их с типом файла test.html. Проверим контекст файла можно командой ls -Z. ls -Z /var/www/html/test.html Изменим 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. 9): chcon -t samba\_share\_t /var/www/html/test.html ls -Z /var/www/html/test.html

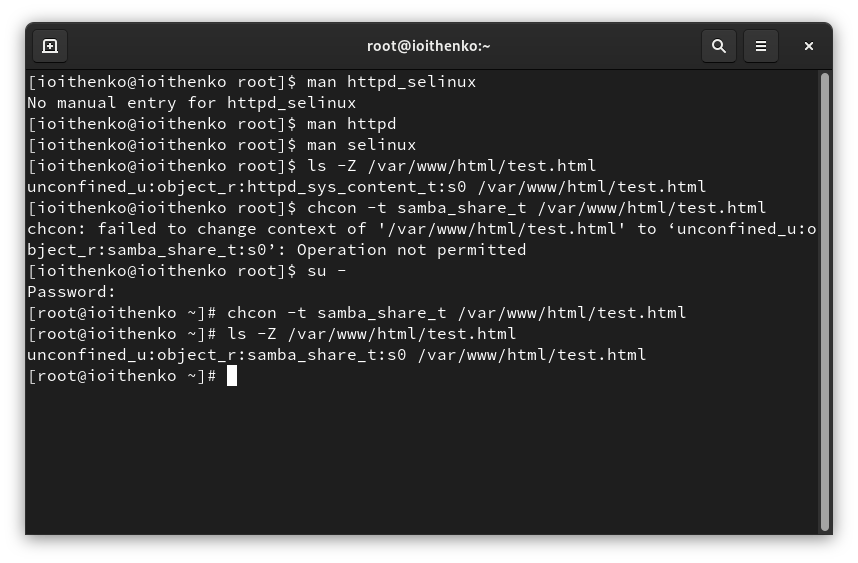


Рис. 9: Изменение контекста

После этого проверим, что контекст поменялся. Попробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html (рис. 10).

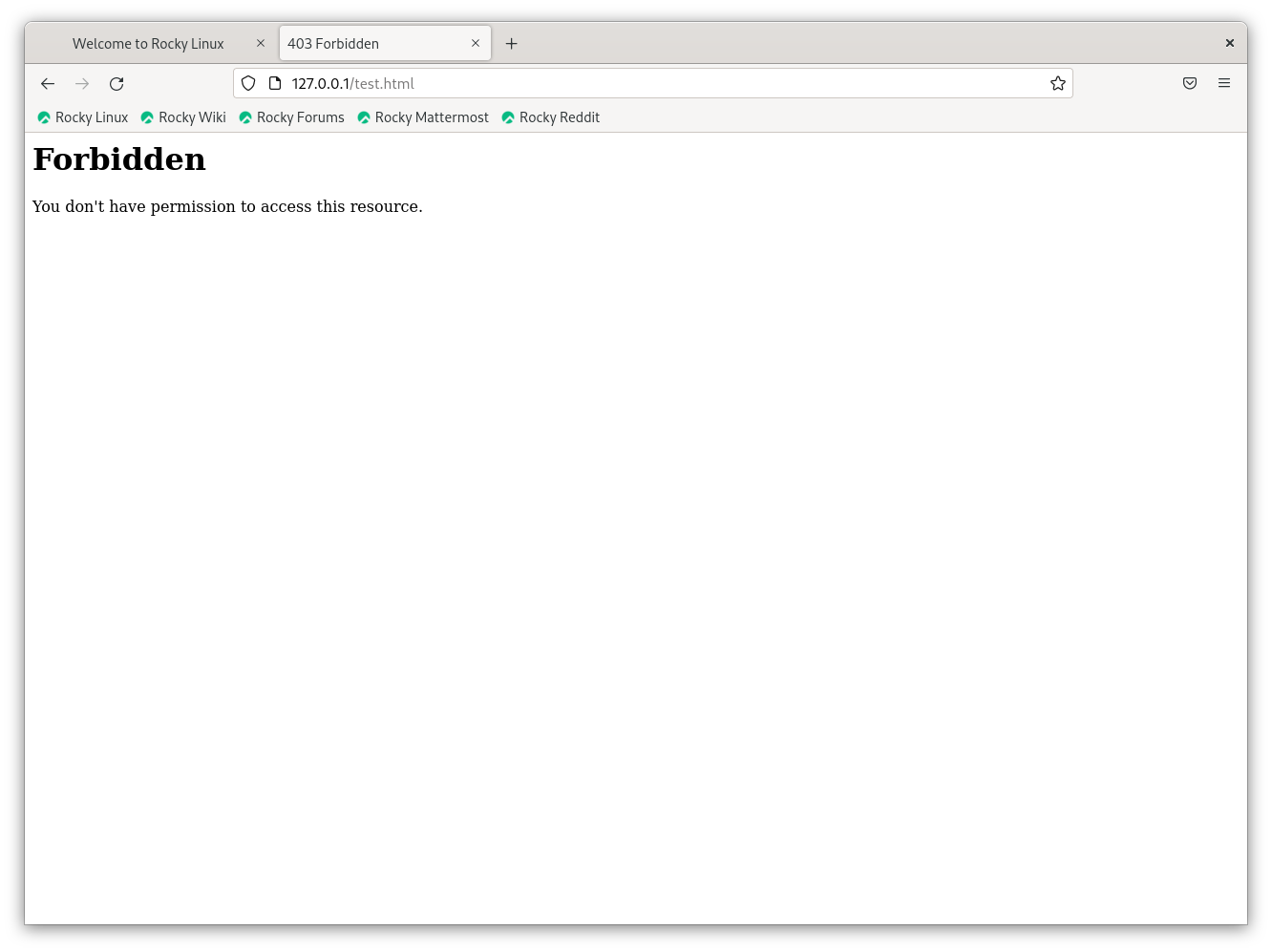


Рис. 10: Проверка отображения файла

ls -l /var/www/html/test.html Просмотрим log-файлы веб-сервера Apache. Также просмотрим системный лог-файл (рис. 11): tail /var/log/messages

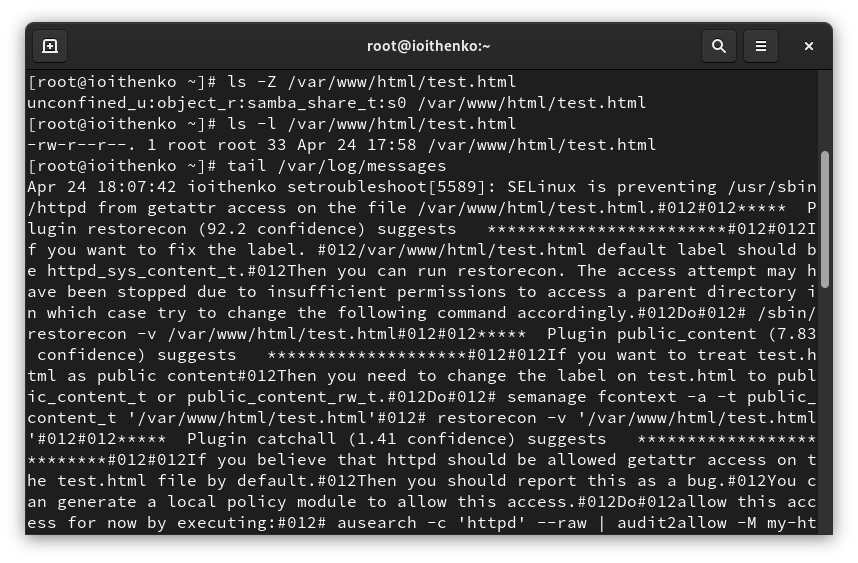


Рис. 11: Лог-файл

Если в системе окажутся запущенными процессы setroubleshootd и audtd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log. Проверим это утверждение самостоятельно (рис. 12).

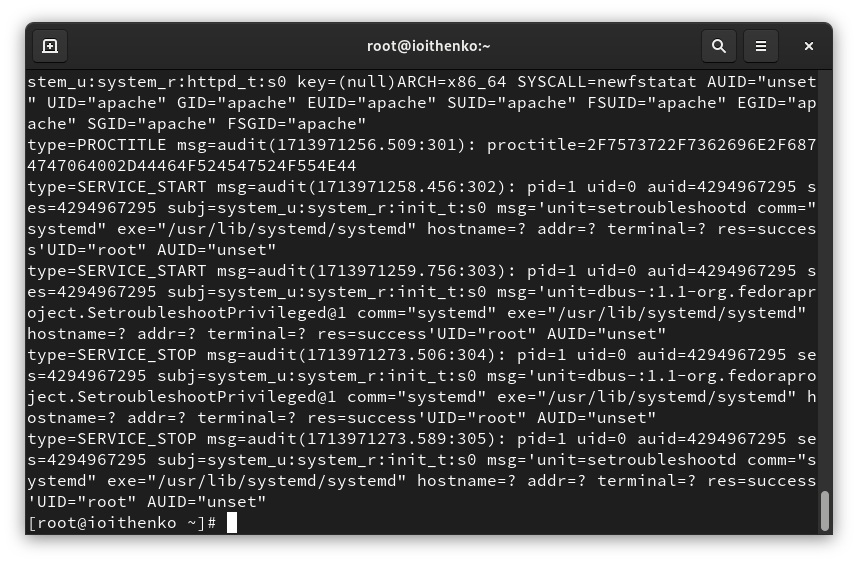


Рис. 12: /var/log/audit/audit.log

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 найдите строчку Listen 80 и заменим её на Listen 81 (рис. 13).

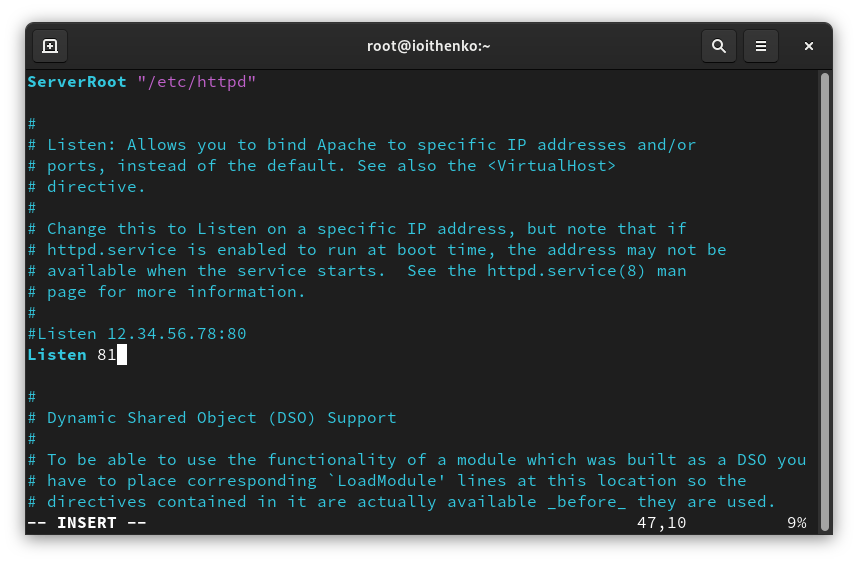


Рис. 13: Замана порта

Выполним перезапуск веб-сервера Apache. Сбой не произошел, так как порт существует.

Проанализируем лог-файлы (рис. 14): tail -n1 /var/log/messages

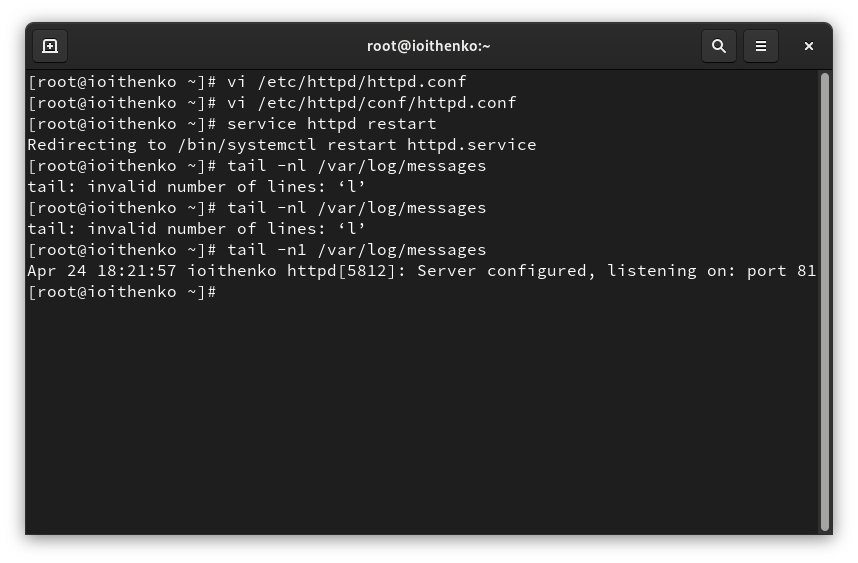


Рис. 14: Лог-файл

Просмотрим файлы /var/log/http/error\_log (рис. 15), /var/log/httpd/access\_log (рис. 16) и /var/log/audit/audit.log (рис. 17).

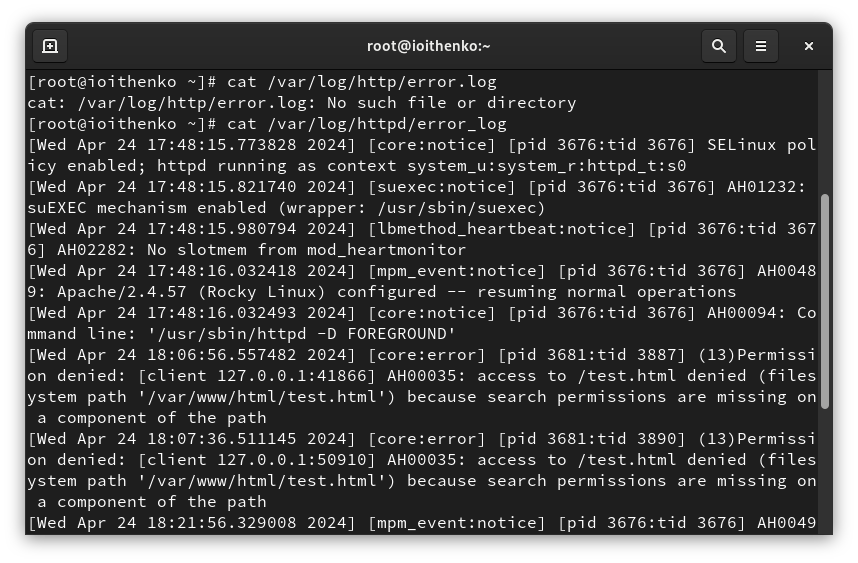


Рис. 15: /var/log/httpd/error\_log

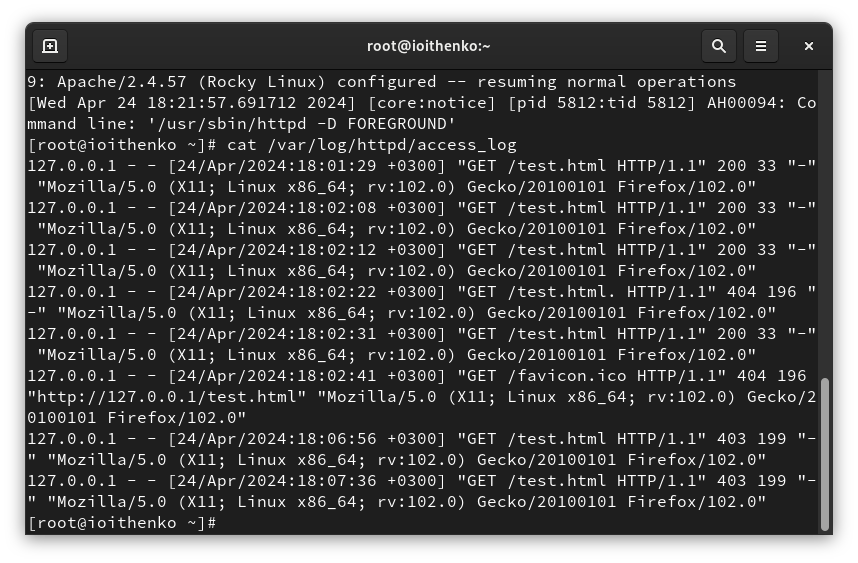


Рис. 16: /var/log/httpd/access\_log

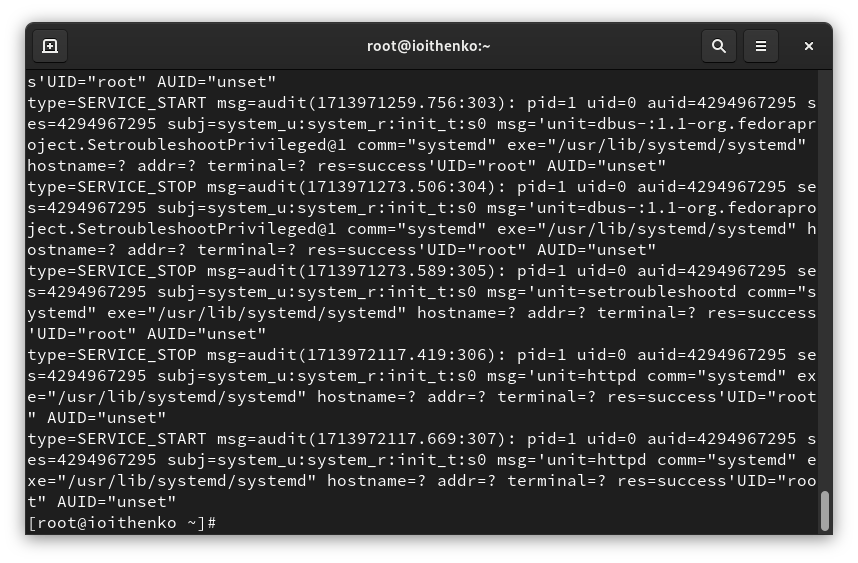


Рис. 17: /var/log/audit/audit.log

Выполним команду semanage port -a -t http\_port\_t -р tcp 81 После этого проверим список портов командой semanage port -l | grep http\_port\_t Попробуем запустить веб-сервер Apache ещё раз. Вернем контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html (рис. 18): chcon -t httpd\_sys\_content\_t /var/www/html/test.html

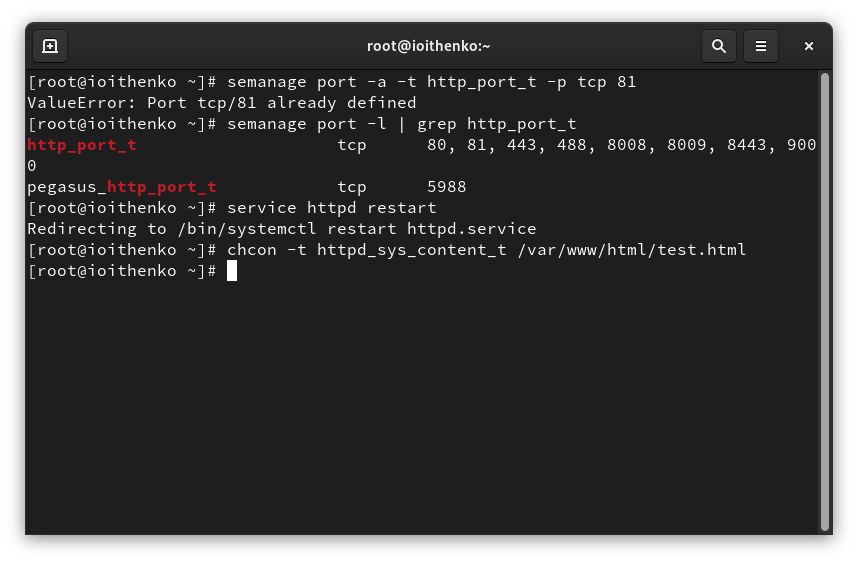


Рис. 18: Контескт

После этого попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html (рис. 19).

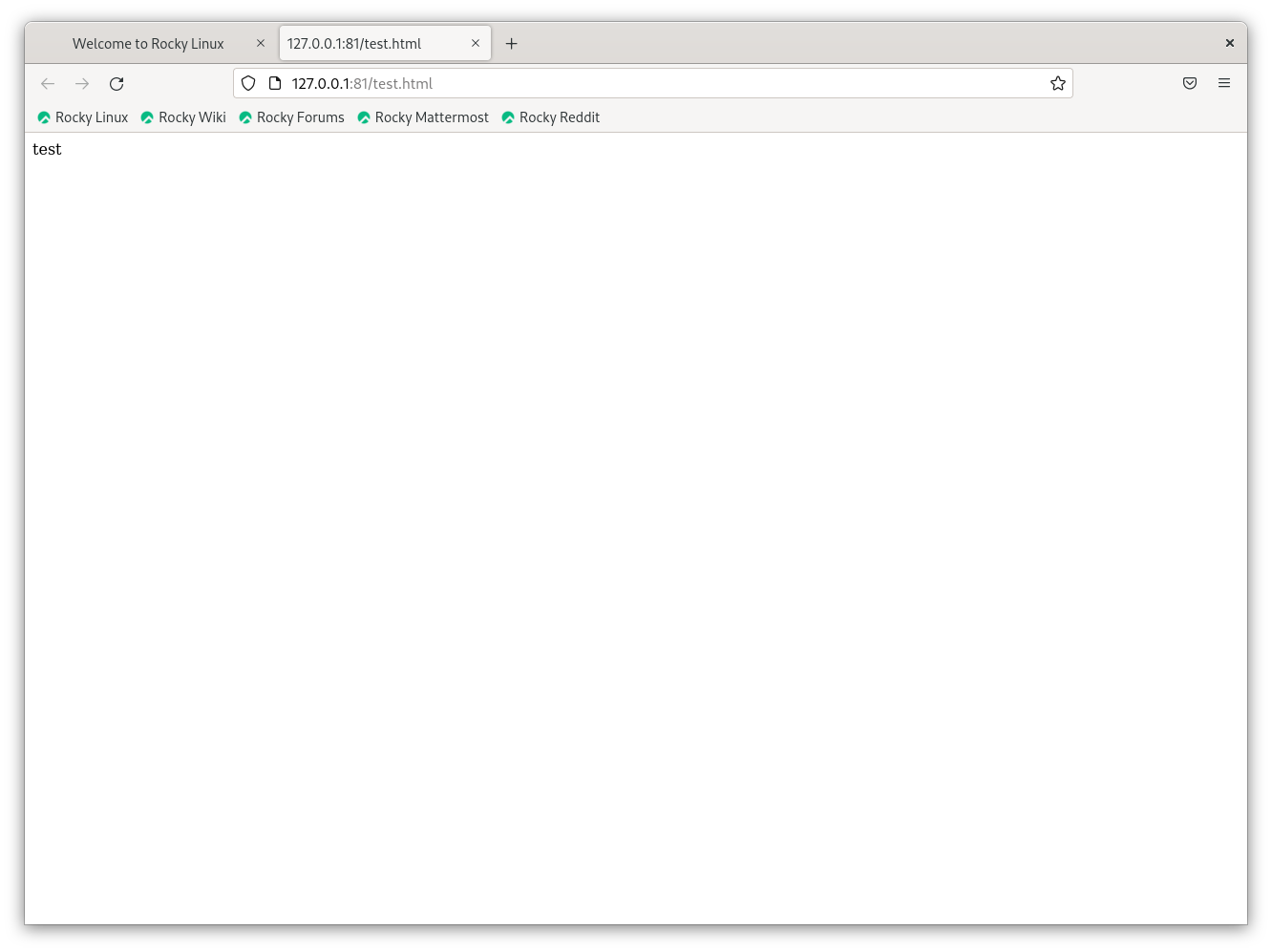


Рис. 19: Проверка отображения файла

Исправим обратно конфигурационный файл apache, вернув Listen 80 (рис. 20).

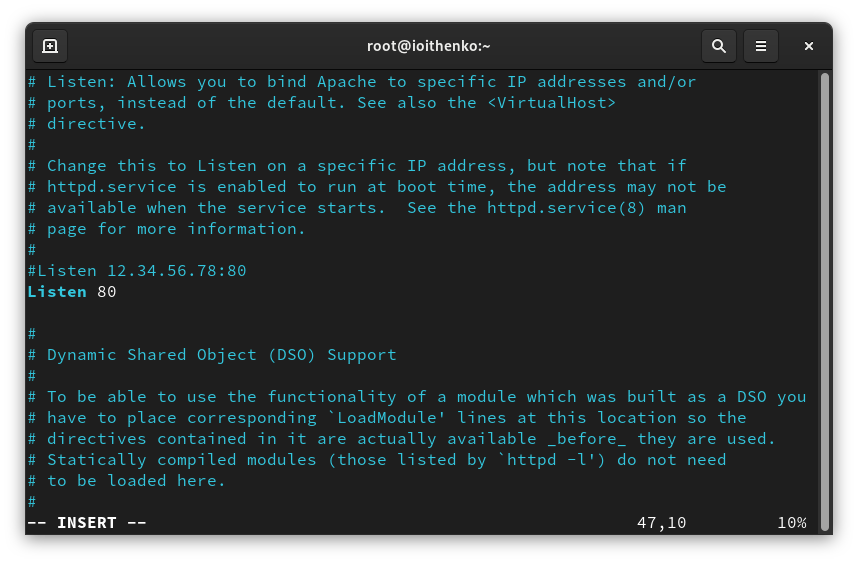


Рис. 20: Возвращение исходной конфигурации

Удалим привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 Удаление не произошло.

Удалим файл /var/www/html/test.html (рис. 21): rm /var/www/html/test.html

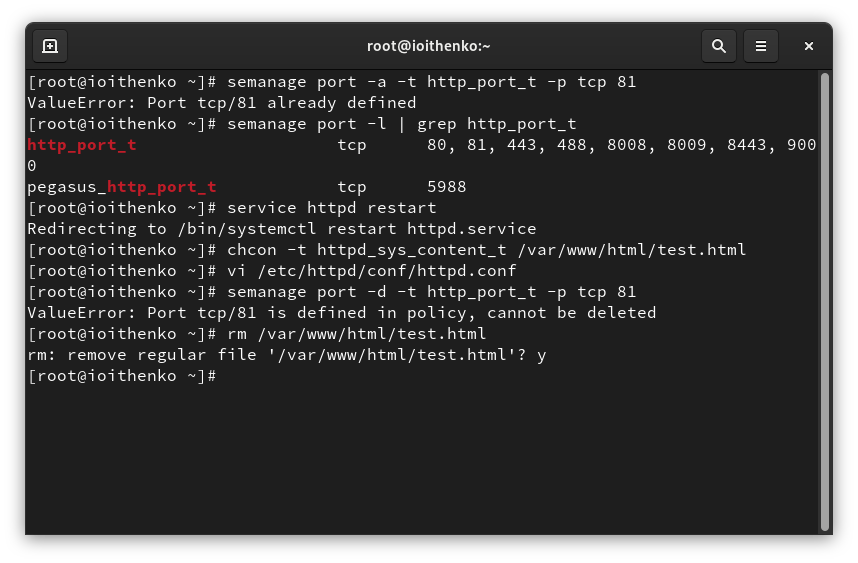


Рис. 21: Удаление привязки к порту и файла

# 3 Выводы

В ходе лабораторной работы я развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. Кулябов Д.С., Королькова А.В., Геворкян М.Н. Информационная безопасность компьютерных сетей. Лабораторные работы, учебное пособие. Москва: РУДН, 2015. 64 с.