Отчёт по лабораторной работе №6

Дисциплина: Основы информационной безопасности

Мишина Анастасия Алексеевна

Содержание

# 1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое прак- тическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache [1].

# 2 Выполнение лабораторной работы

Открываем терминал и убеждаемся, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus. Запустим веб-сервер и убедимся, что он работает: service httpd start и service httpd status (рис. 1).

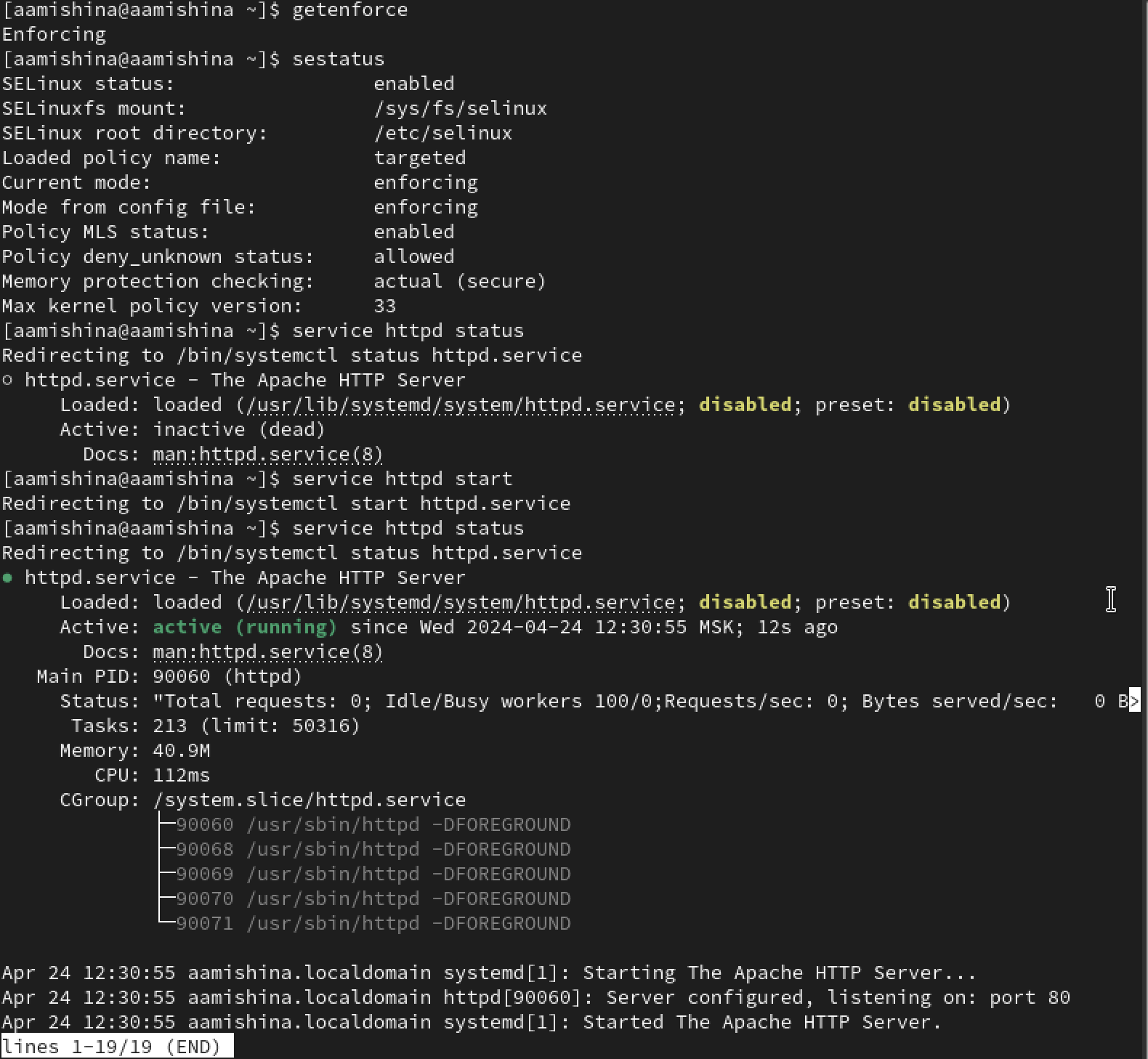


Рис. 1: Проверка режима SELinux, запуск веб-сервера

Определим контекст безопасности веб-сервера: ps auxZ | grep httpd. Посмотрим текущее состояние переключателей SELinux для Apache с помощью команды: sestatus -bigrep httpd. Обратим внимание, что многие из них находятся в положении «off» (рис. 2).

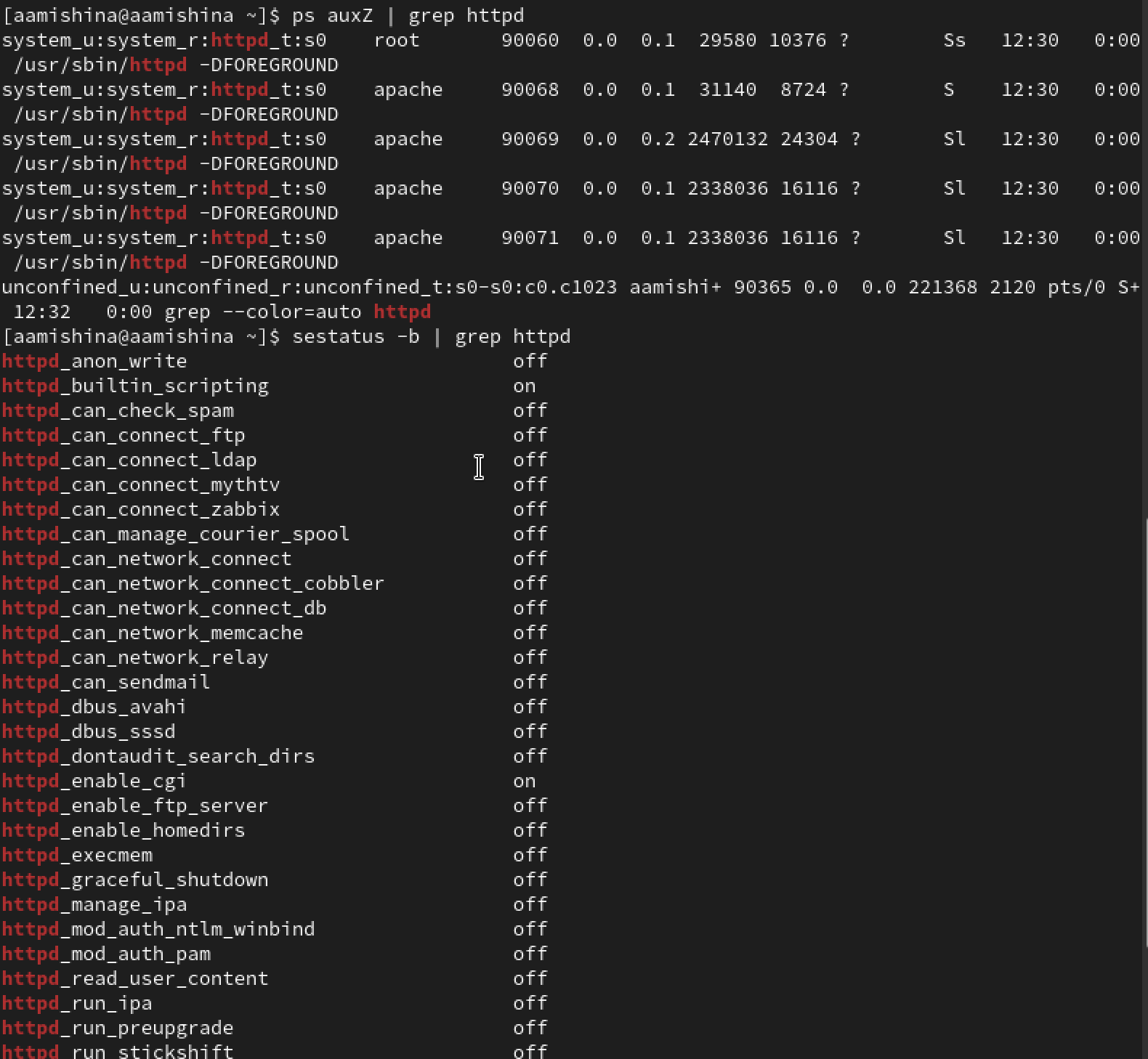


Рис. 2: Контекст безопасности веб-сервера и состояние переключателей SELinux

Посмотрим статистику по политике с помощью команды seinfo, также определим множество пользователей, ролей, типов (рис. 3).

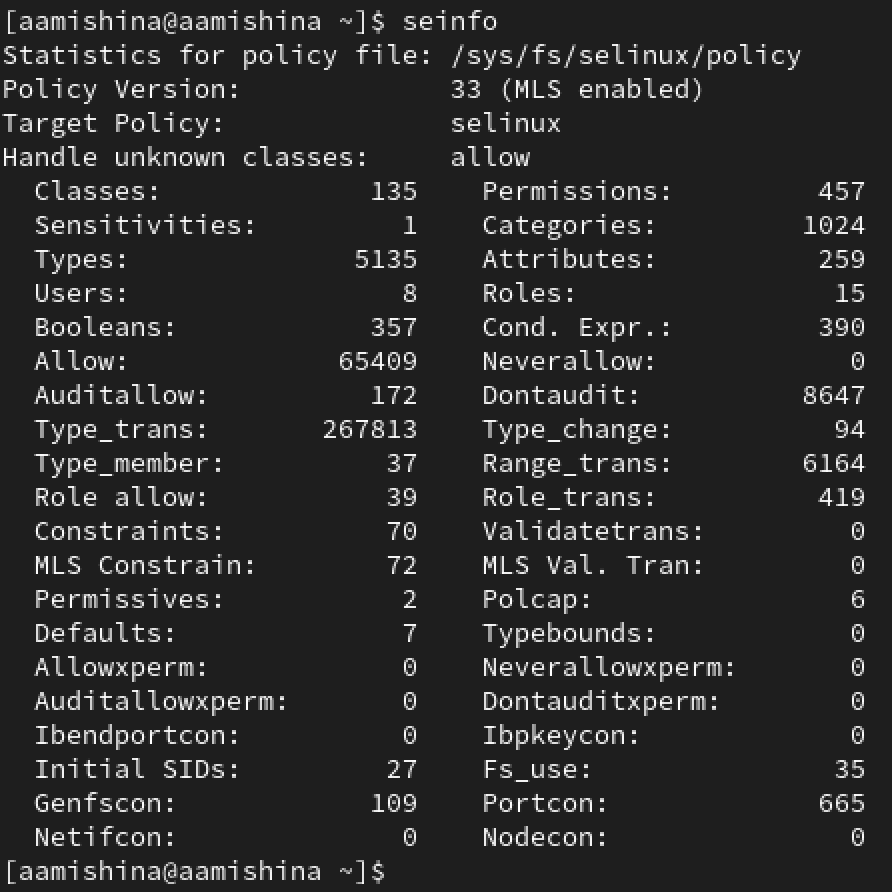


Рис. 3: Статистика по политике

Определяем тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www. Определяем тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html. Определяем круг пользователей, которым разрешено создание файлов в директории /var/www/html (рис. 4). Создаем от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html (рис. 5).

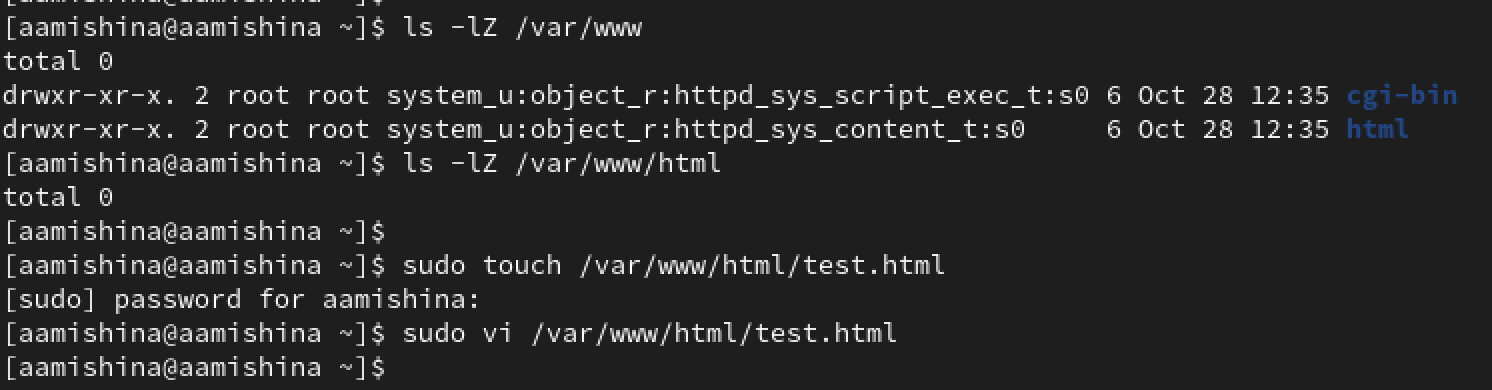


Рис. 4: Определение типов файлов и поддиректорий www и html. Создание файла test.html

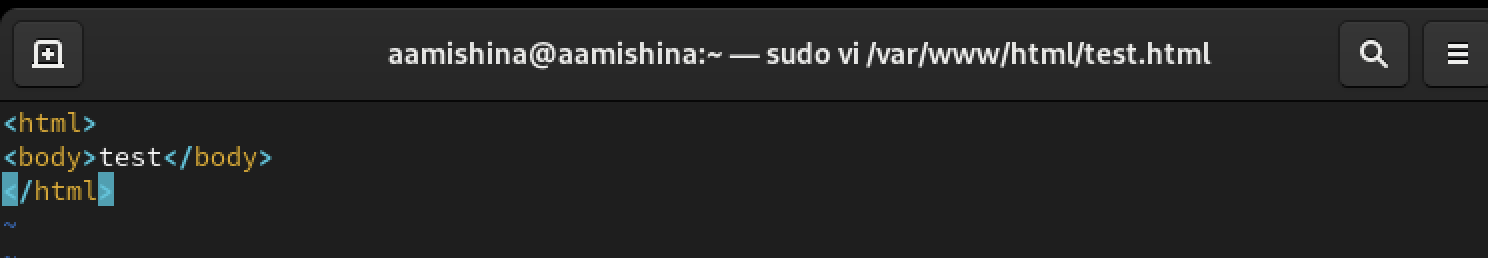


Рис. 5: Файл test.html

Проверяем контекст созданного файла (рис. 6).



Рис. 6: Контекст файла test.html

Обратимся к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убеждаемся, что файл был успешно отображён (рис. 7).

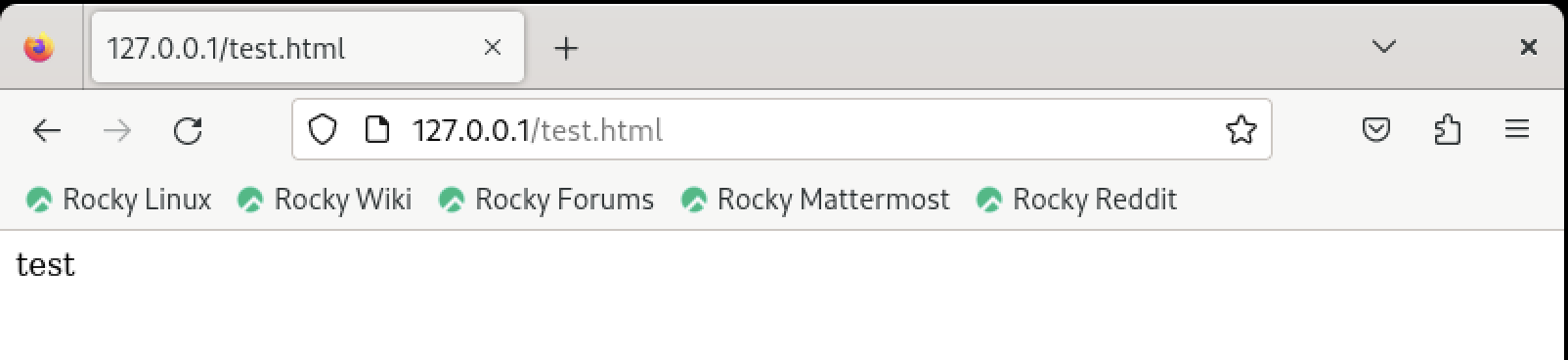


Рис. 7: Запуск файла в браузере

Изучаем справку man httpd и man selinux. Проверяем контекст файла можно командой ls -Z, т.е. ls -Z /var/www/html/test.html (рис. 8).



Рис. 8: Изучение справок, контекст файла test.html

Сменим 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: chcon -t samba\_share\_t /var/www/html/test.html, проверим, что контекст поменялся: ls -Z /var/www/html/test.html (рис. 9).

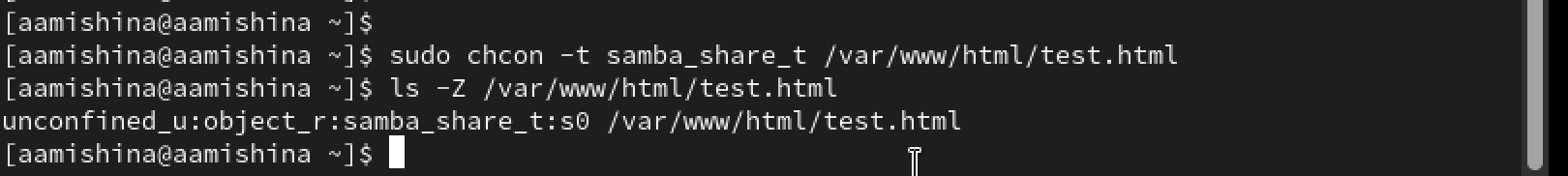


Рис. 9: Смена контекста файла, проверка

Попробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получаем сообщение об ошибке: Forbidden You don’t have permission to access /test.html on this server (рис. 10).

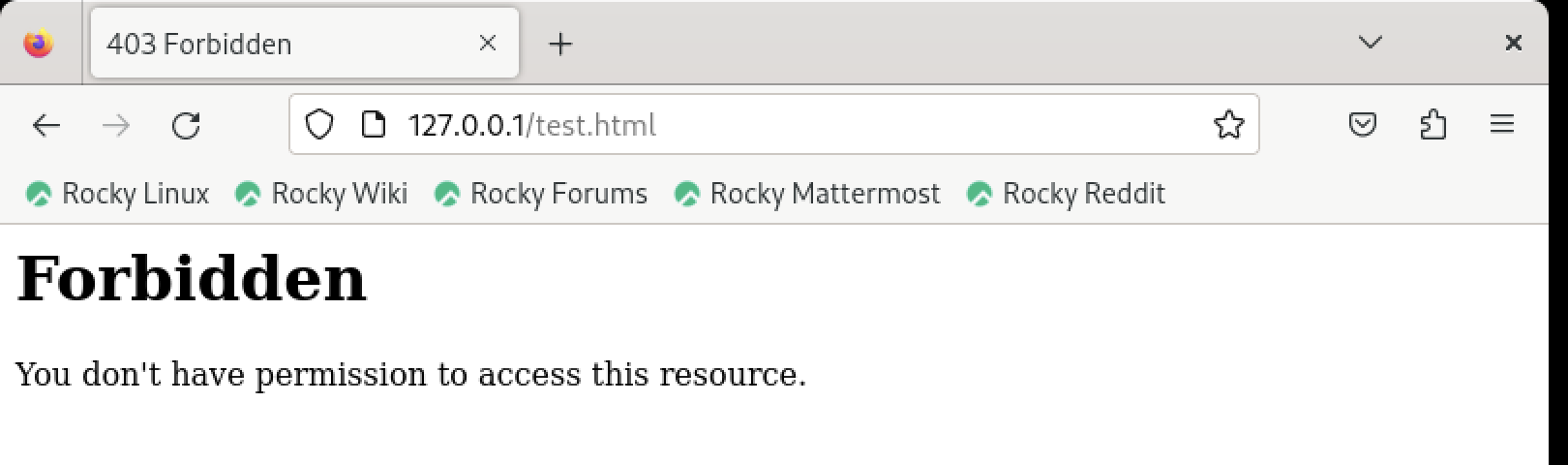


Рис. 10: Попытка просмотра

Смотрим права доступа на файл ls -l /var/www/html/test.html, также смотрим системный log-файл tail /var/log/messages (рис. 11).

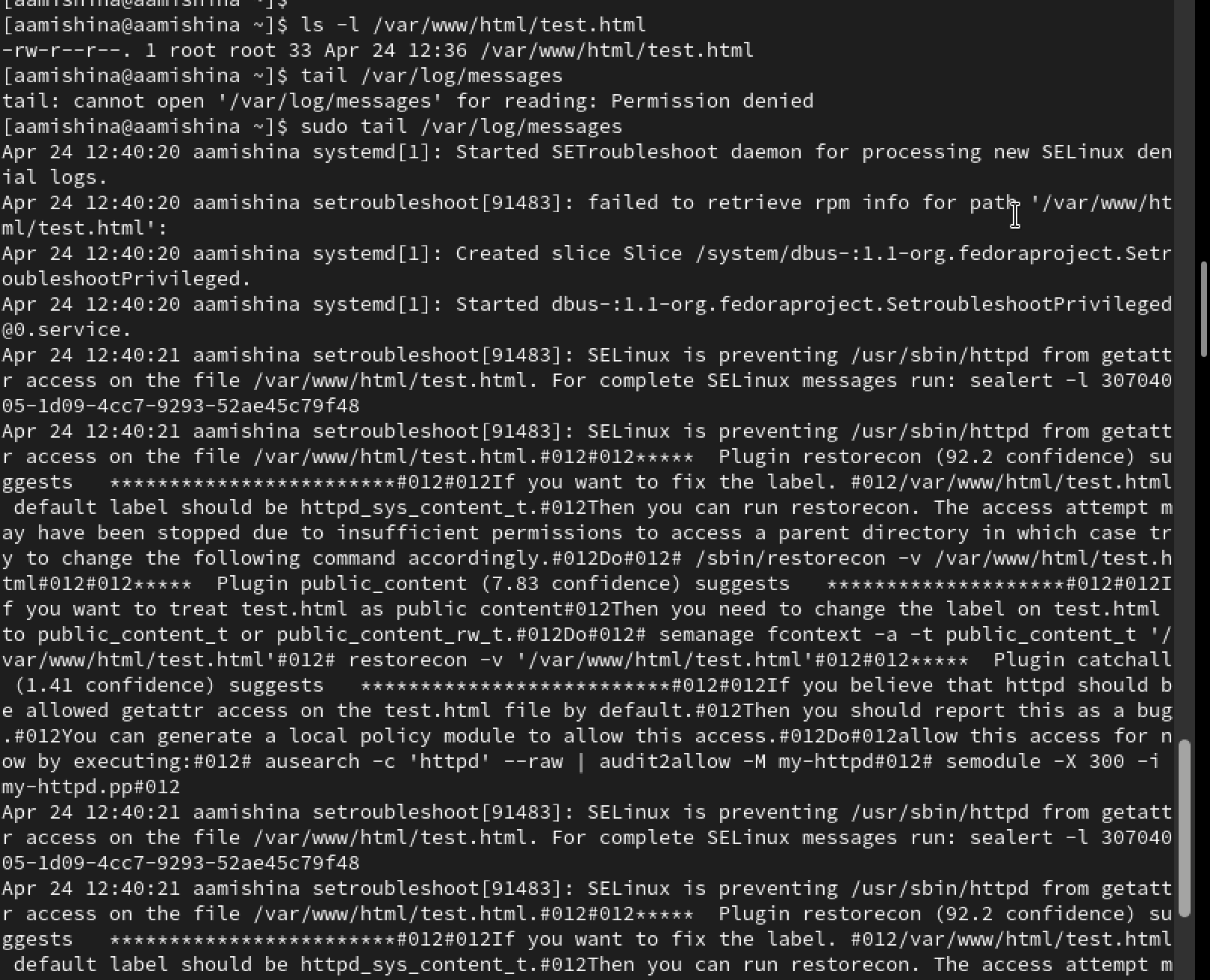


Рис. 11: Права доступа, системный log-файл

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 находим строчку Listen 80 и меняем её на Listen 81 (рис. 12).

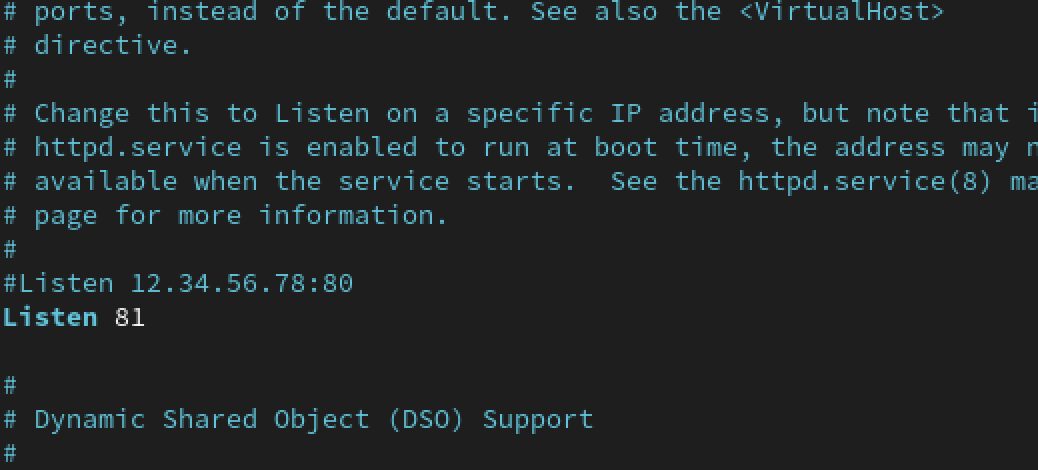


Рис. 12: Файл httpd.conf

Выполняем перезапуск веб-сервера Apache (рис. 13). Происходит сбой (рис. 14).

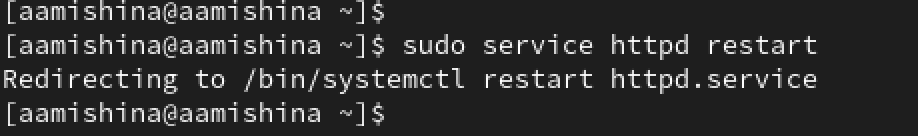


Рис. 13: Перезапуск веб-сервера Apache

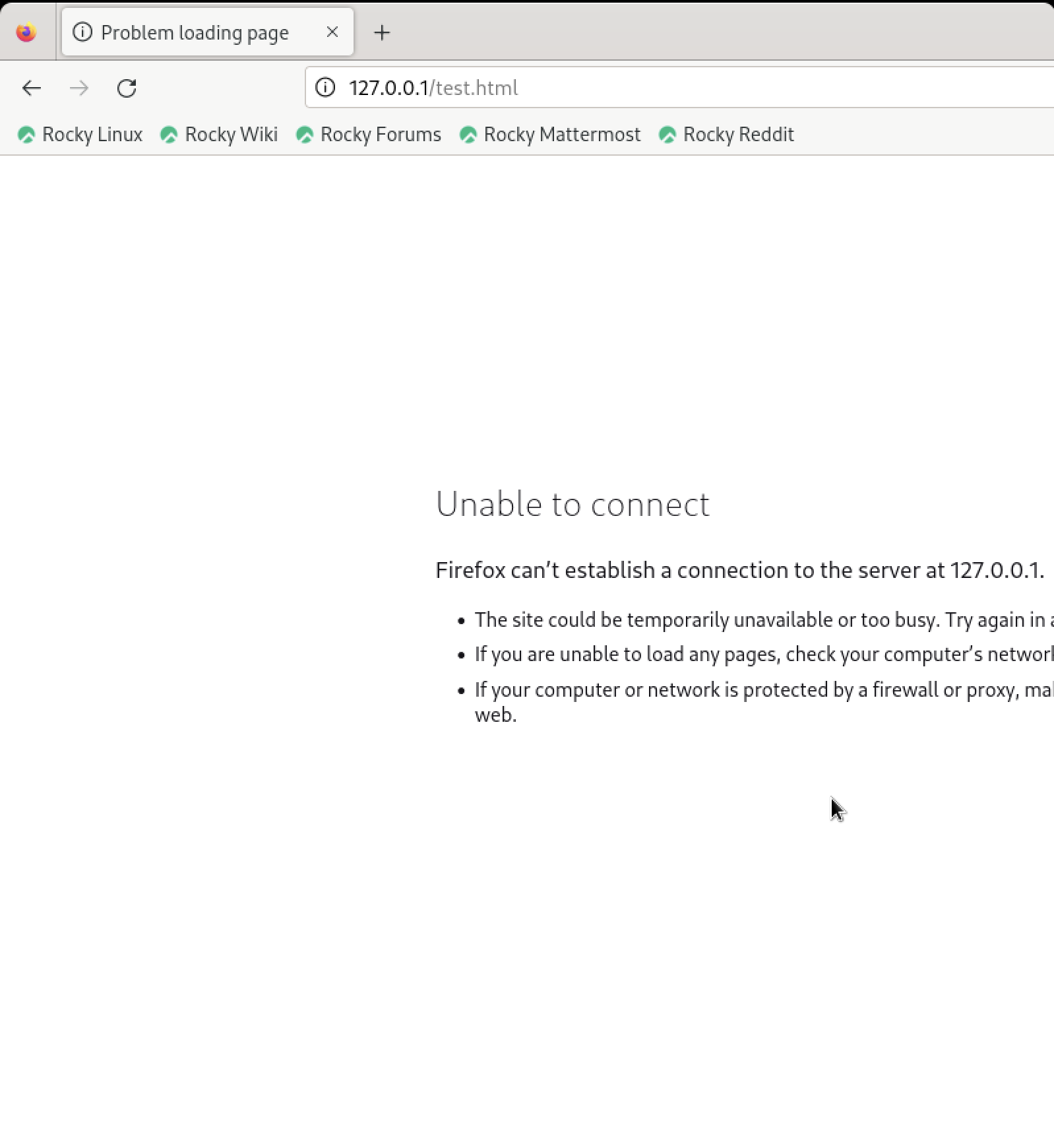


Рис. 14: Сбой веб-сервера

Анализируем лог-файлы: tail -nl /var/log/messages (рис. 15. Просматриваем файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log (рис. 16.

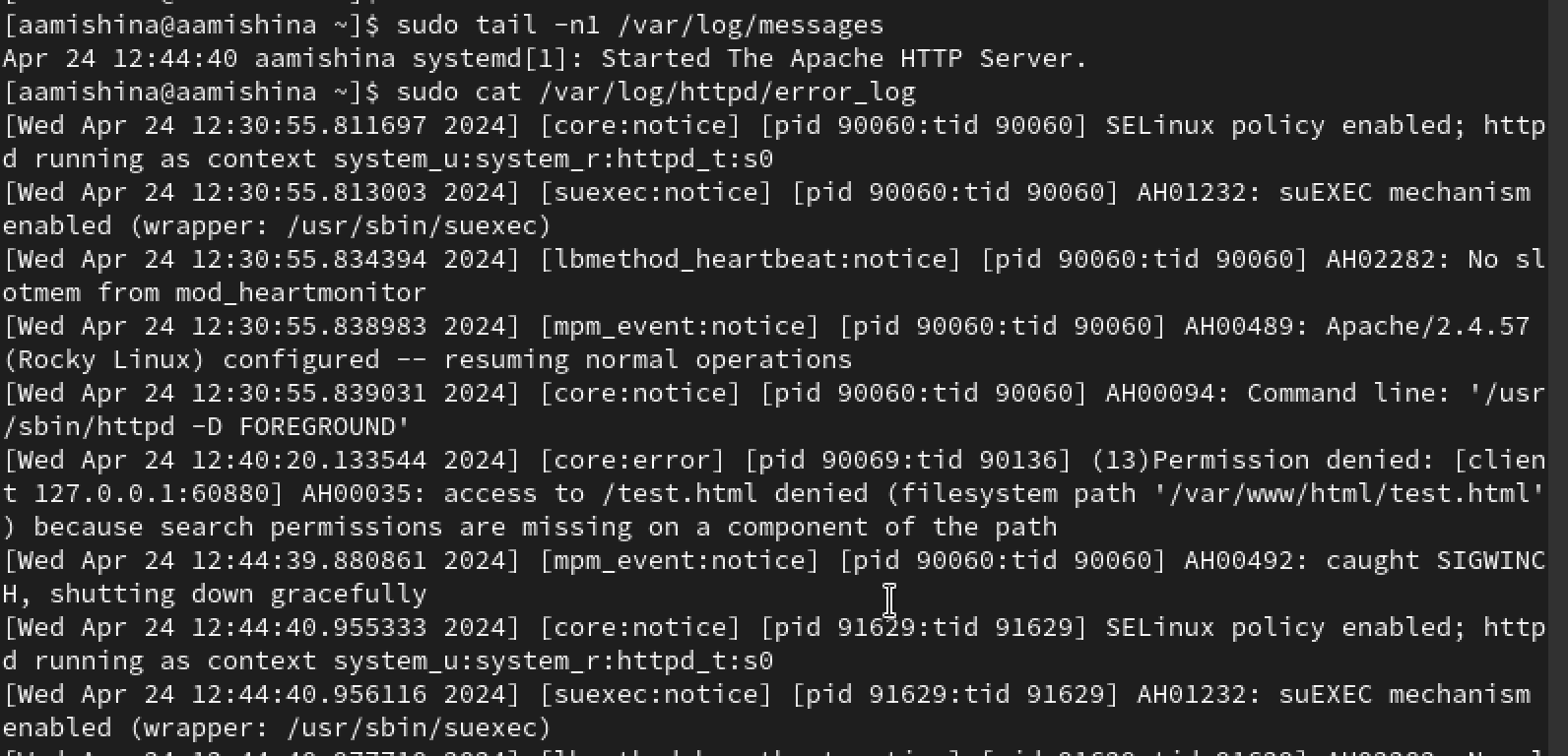


Рис. 15: Просмотр лог-файлов

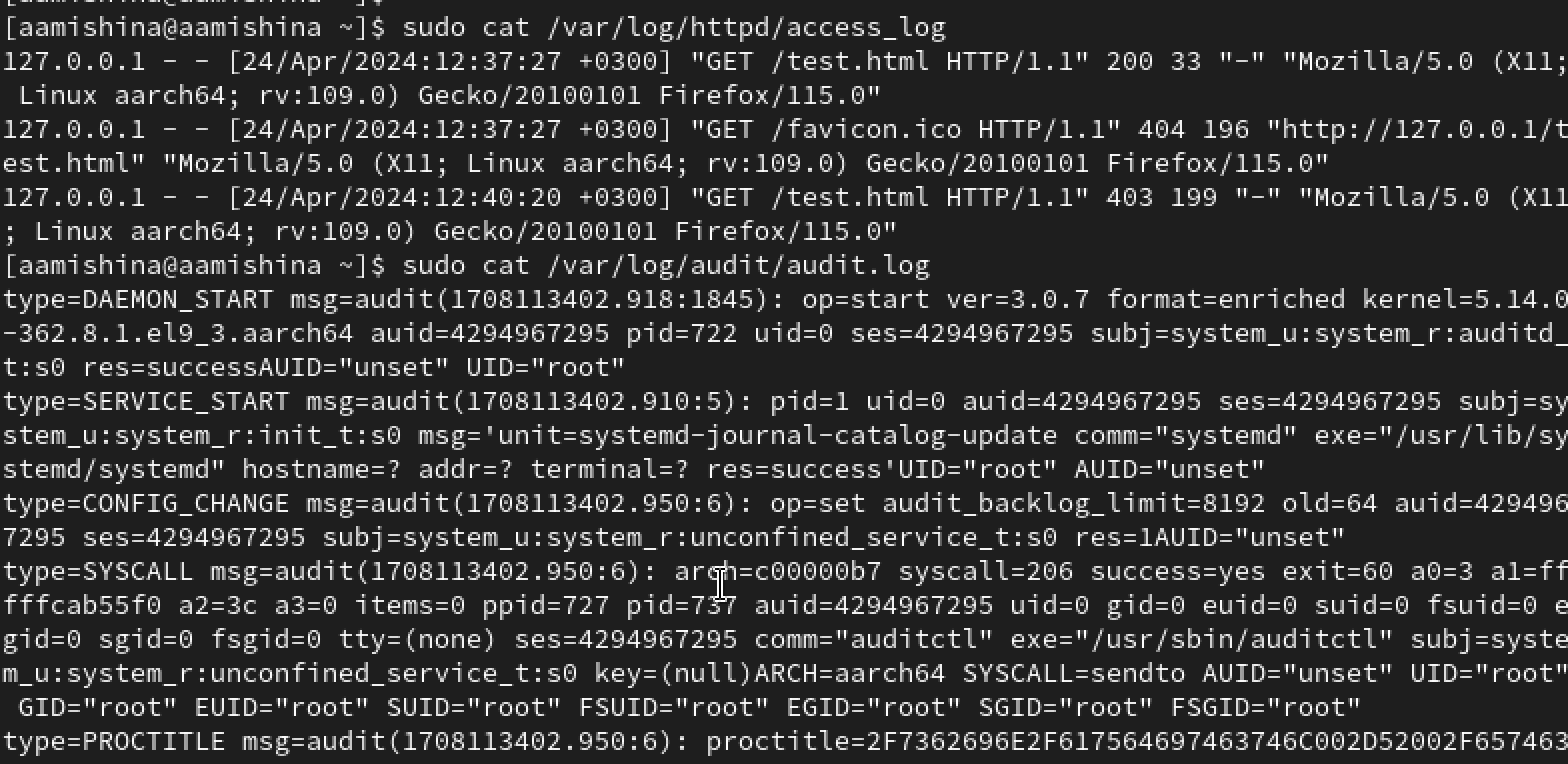


Рис. 16: Просмотр лог-файлов

Выполняем команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверяем список портов командой semanage port -l | grep http\_port\_t. Убеждаемся, что порт 81 появился в списке. Перезагружаем веб-сервер еще раз. Возвращаем контекст httpd\_sys\_cоntent\_t к файлу /var/www/html/test.html: chcon -t httpd\_sys\_content\_t /var/www/html/test.html (рис. 17.



Рис. 17: Проверка списка портов, перезагрука сервера, возвращение контекста

После этого попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Видим содержимое файла — слово «test» (рис. 18.

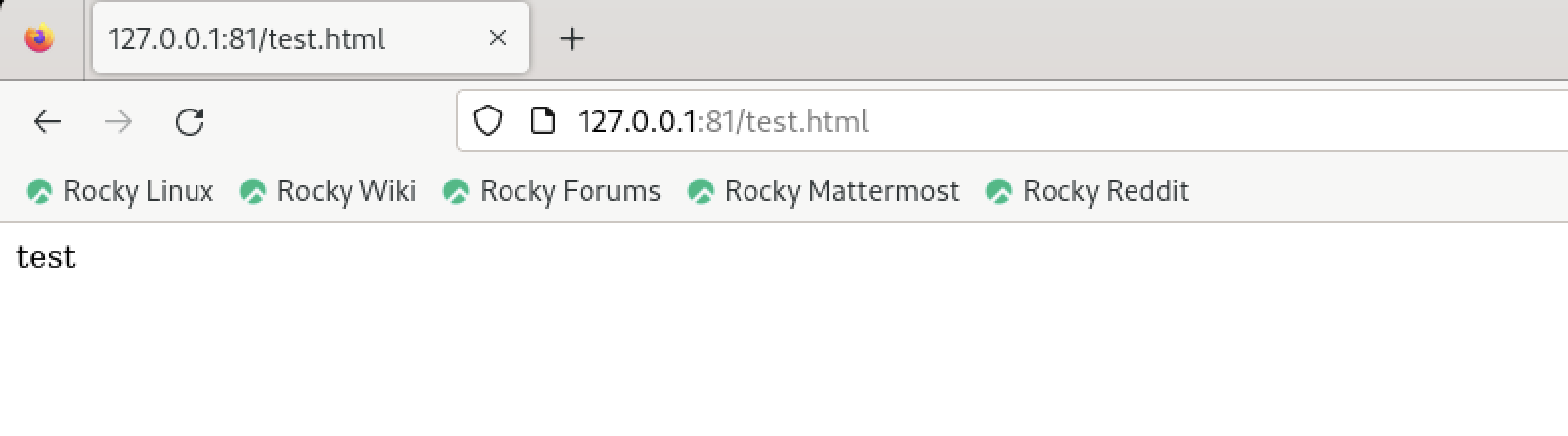


Рис. 18: Просмотр файла через сервер

Исправляем обратно конфигурационный файл apache, вернув Listen 80 (рис. 19.

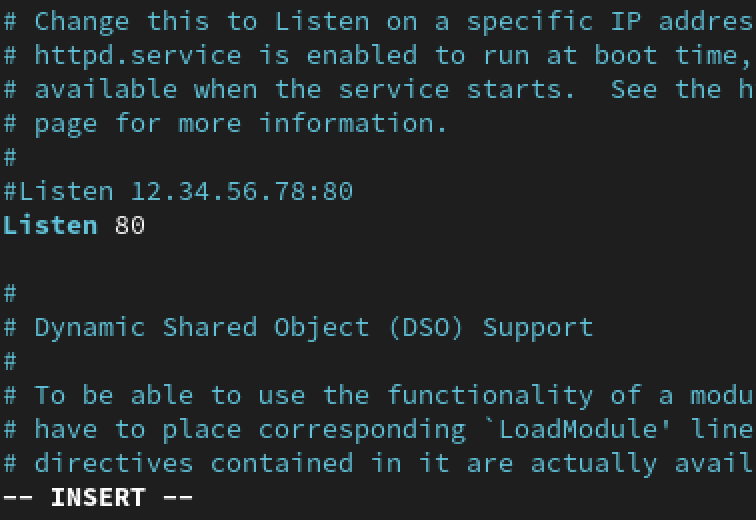


Рис. 19: Файл httpd.conf

Удалим привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и проверим, что порт 81 удалён. Удаляем файл var/www/html/test.html: rm /var/www/html/test.html (рис. 20.

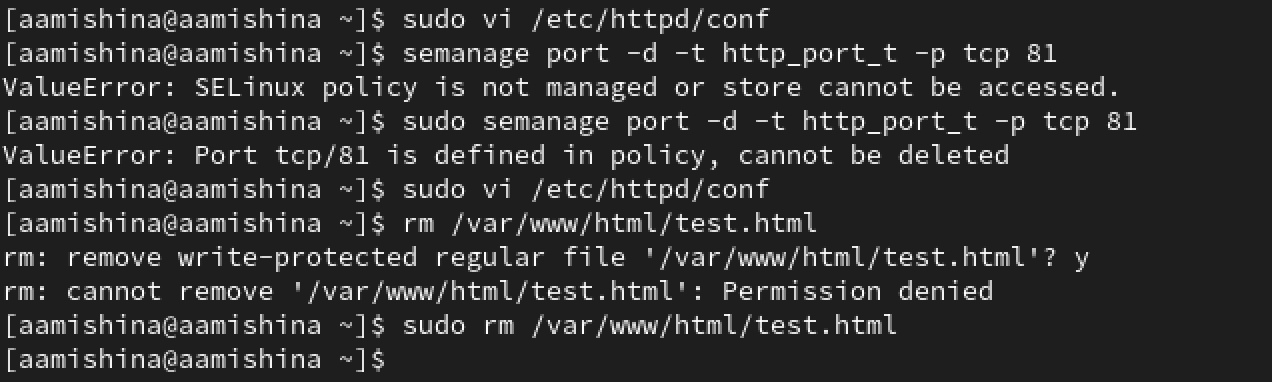


Рис. 20: Удаляем привязку http\_port\_t к 81, выполняем проверку, удаляем файл test.html

# 3 Выводы

В ходе выполнения данной лабораторной работы, я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux1, а также 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.