Отчёт по лабораторной работе

Лабораторная №6

Дерябина Мария Сергеевна

Содержание

# Цель работы

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

# Подготовка лабораторного стенда

Для выполнения работы, установила веб-сервер Apache (рис. 1).

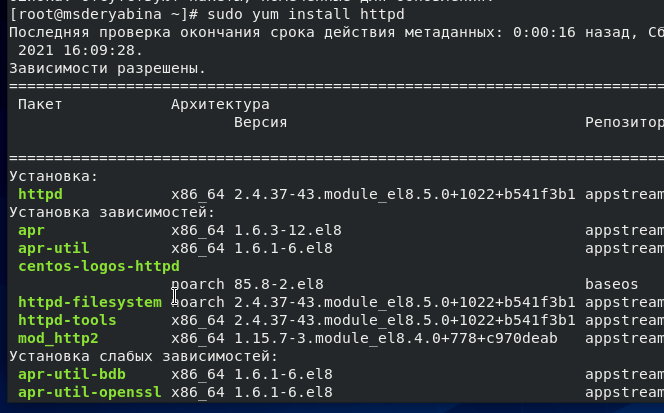


Figure 1: Установка Apache

В конфигурационном файле /etc/httpd/conf/httpd.conf задала параметр ServerName

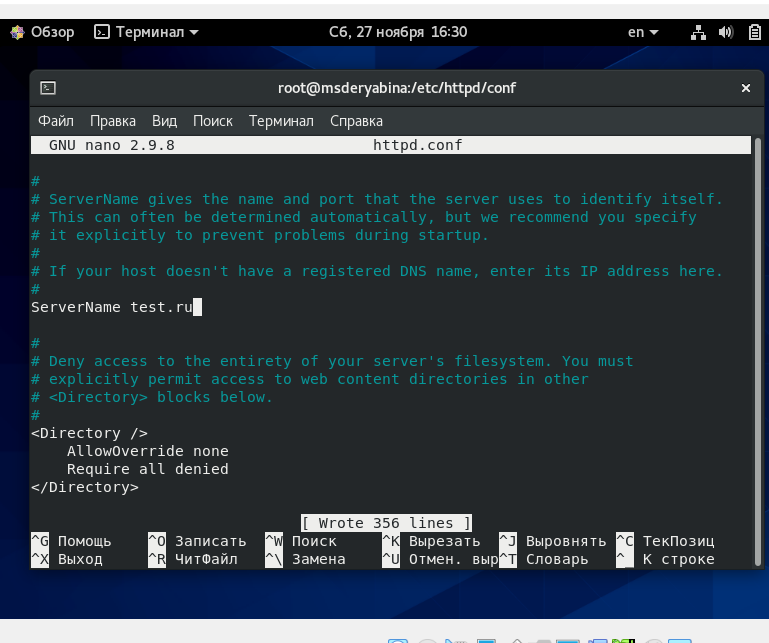


Figure 2: Конфигурационный файл httpd.conf

Отключила пакетный фильтр (../image/3.png){#fig:003 width=70%}

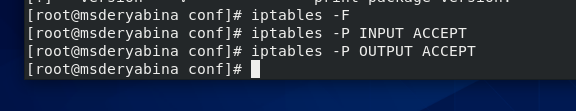


Figure 3: Отключение пакетного фильтра

# Выполнение лабораторной работы

## Изучение политики и контектса SELinux

Вошла в систему и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus (рис. 4).

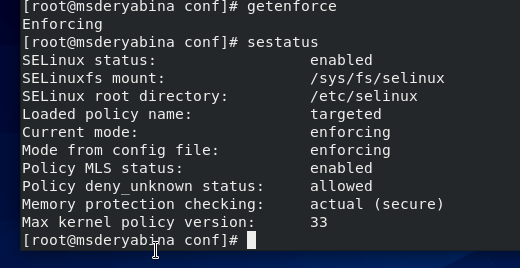


Figure 4: Статус SELinux

Запустила веб-сервер Apache. (рис. 5).

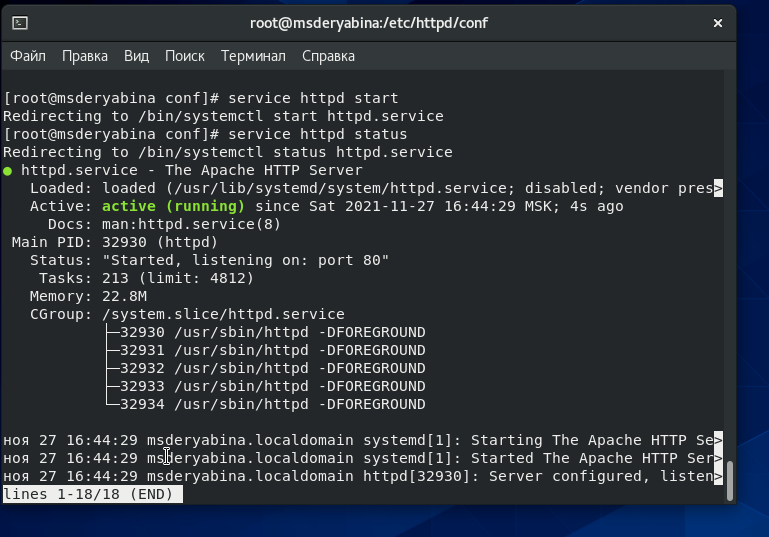


Figure 5: Старт веб-сервера Apache

Нашла веб-сервер в списке процессов. Его контекст безопасности - “system\_u:system:r:httpd\_t:s0” (рис. 6).

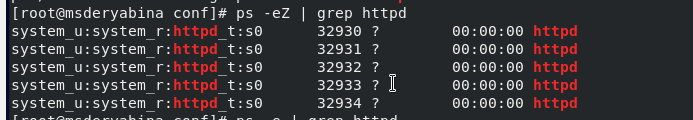


Figure 6: Контекст безопасности веб-сервера Apache

Посмотрела текущее состояние переключателей SELinux для Apache. Многие их них отключены (рис. 7).

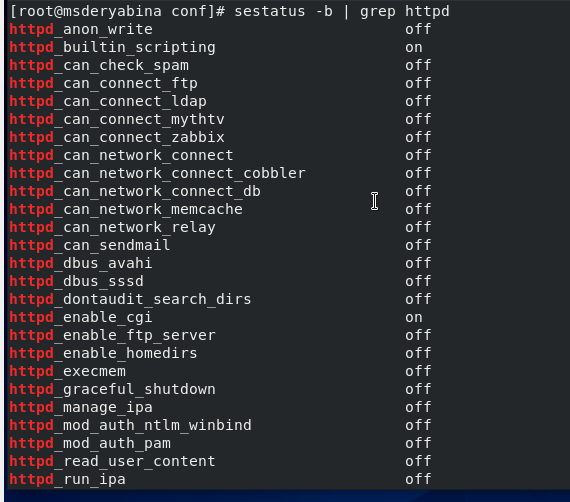


Figure 7: Состояние переключателей SELinux для Apache

Посмотрела статистику по политике. Количество пользователей - 8, ролей - 14, типов - 4934 (рис. 8).

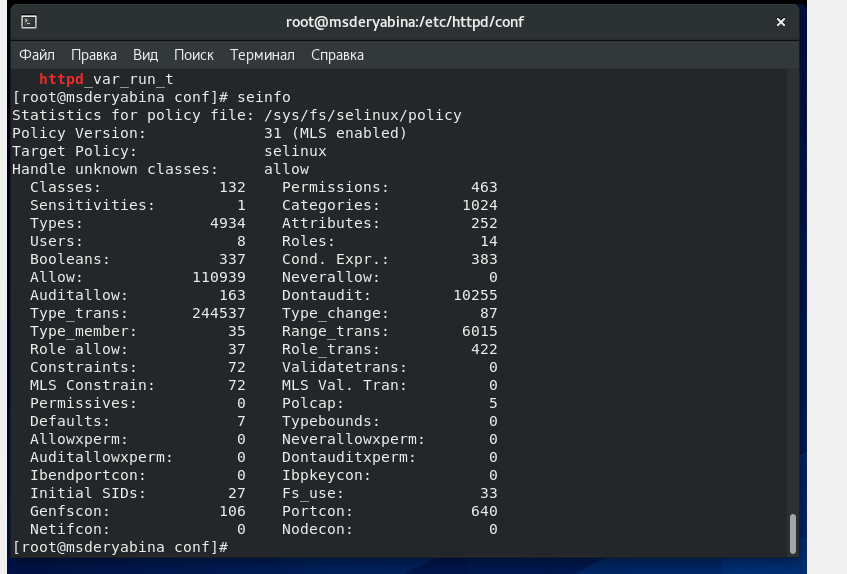


Figure 8: Статистика по политике SELinux

Определила тип поддиректорий, находящихся в директории /var/www. Тип каталога cgi-bin - httpd\_sys\_script\_exec\_t, тип каталога html - httpd\_sys\_content\_t (рис. 9).



Figure 9: Типы поддиректорий в директории /var/www

Исходя из прав доступа каталога /var/www/html, только суперпользователю разрешено создание файлов в нем. От имени суперпользователя создала файл test.html (рис. 10).

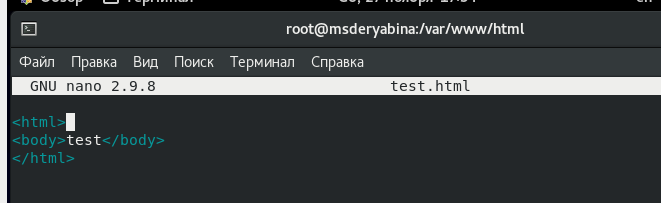


Figure 10: Файл /var/www/html/test.html

Контекст созданного файла - unconfined\_u:object\_r:httpd\_sys\_content\_t:s0. Так как по умолчанию пользователи CentOS являются свободными от типа, созданному файлу test.html был сопоставлен пользователь unconfined\_u. Роль object\_r используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. Тип httpd\_sys\_content\_t позволяет процессу httpd получить доступ к файлу. Благодаря наличию последнего типа можно получить доступ к файлу при обращении к нему через браузер (рис. 11).

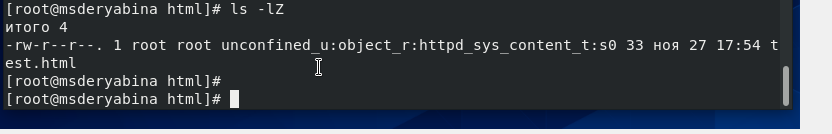


Figure 11: Контекст файла test.html

Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html (рис. 12).

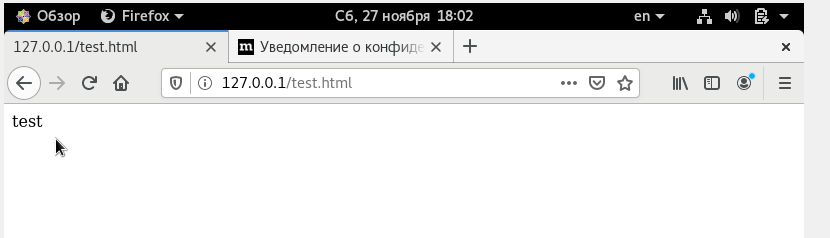


Figure 12: Доступ к файлу test.html через браузер

Изменила контекст файла test.html на samba\_share\_t, к которому процесс httpd не должен иметь доступа (рис. 13).

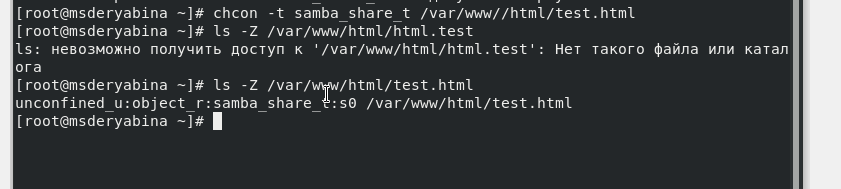


Figure 13: Изменение контекста файла test.html

Снова попробовала получить доступ к файлу через браузер, получила сообщение об ошибке(рис. 14).

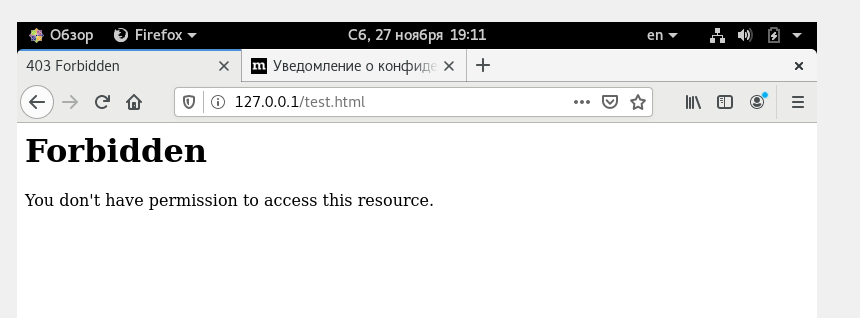


Figure 14: Сообщение об ошибке после смены конекста

Посмотрела лог ошибок веб-сервера Apache и системный лог. В них появились записи о запрете доступа к файлу. В системном логе появилась информация о необходимости сменить тип файла test.html, чтобы демон httpd мог к нему обращаться(рис. 15, рис. 16).

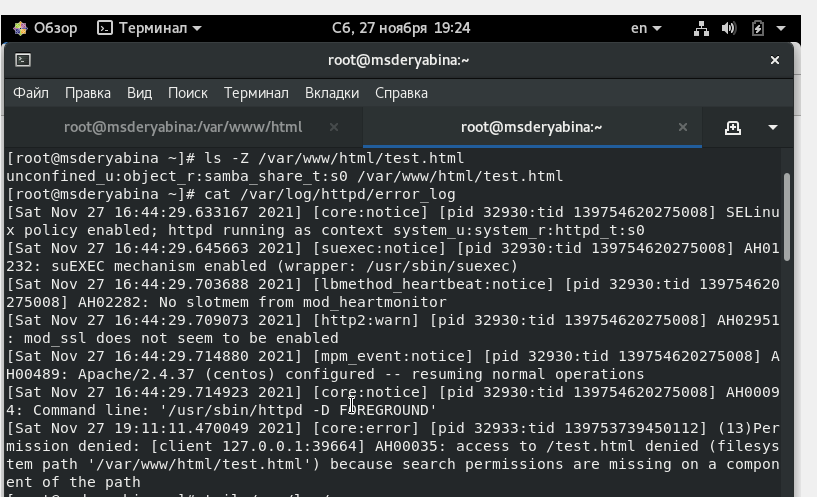


Figure 15: Лог ошибок Apache

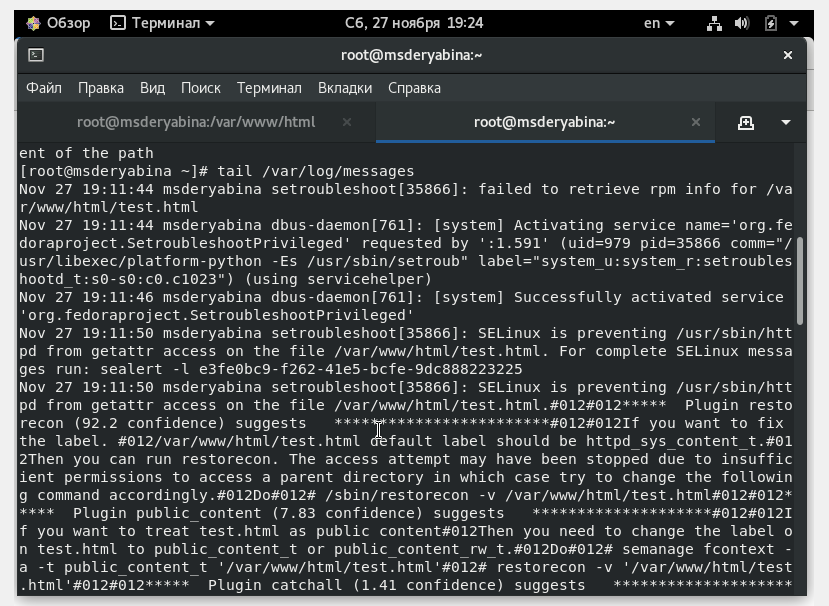


Figure 16: Системный лог-файл

## Изменение TCP-порта

В соотсветствии с новой политикой, порт 81 входит в список портов по умолчанию, поэтому я изменила порт с 80 на 82 в файле /etc/httpd/conf/httpd.conf (рис. 17).

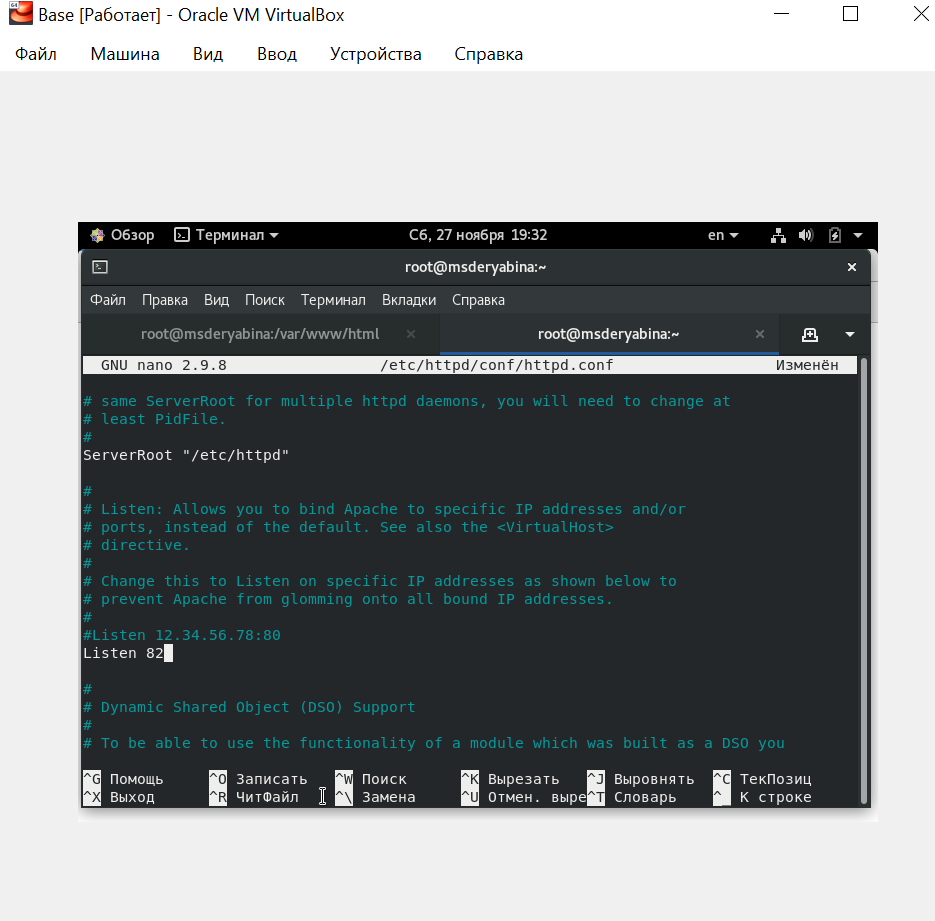


Figure 17: Изменение TCP-порта

При перезапуске веб-сервера произошел сбой. В файле /var/log/messages появилась запись о запрете доступа через порт 82 и необходимости изменить тип порта (рис. 18). В файле /var/log/audit/audit.log появилась запись о неудачной попытке запуска веб-сервера (рис. 19). В файле /var/log/httpd/error\_log есть запись только о завершении работы веб-сервера (рис. 20). В файле /var/log/httpd/access\_log не появилось новых записей (рис. 21).

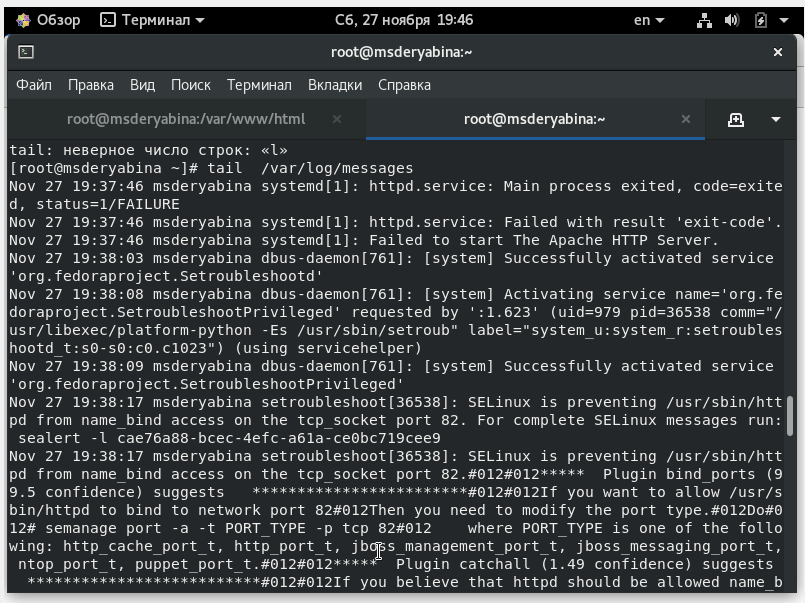


Figure 18: /var/log/messages

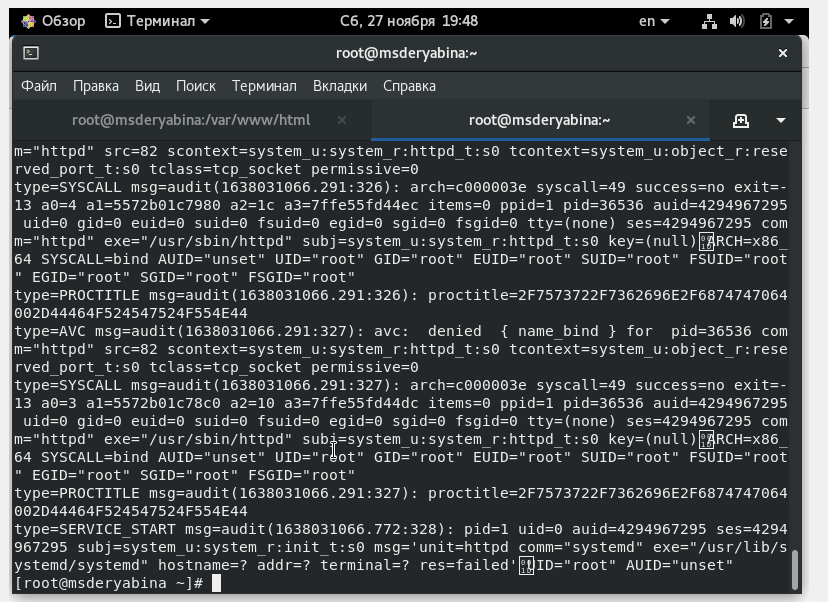


Figure 19: /var/log/audit/audit.log

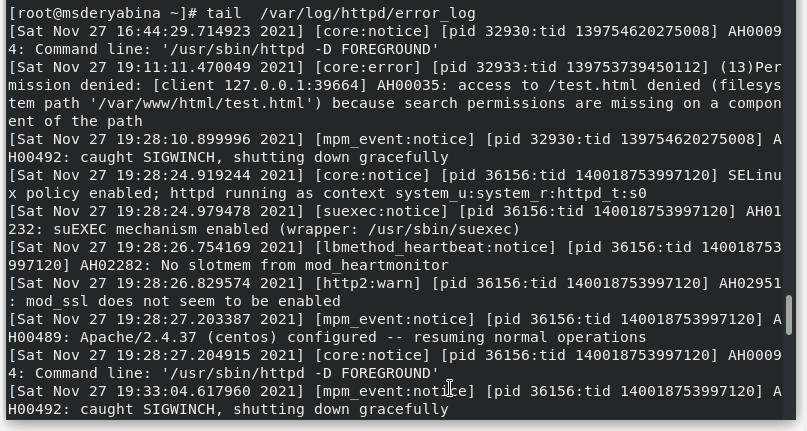


Figure 20: /var/log/httpd/error\_log

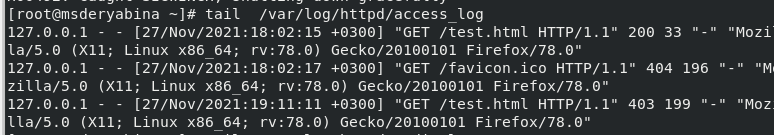


Figure 21: /var/log/httpd/access\_log

Добавила порт 82 к списку портов http\_port\_t. После этого удалось запустить веб-сервер (рис. 22).

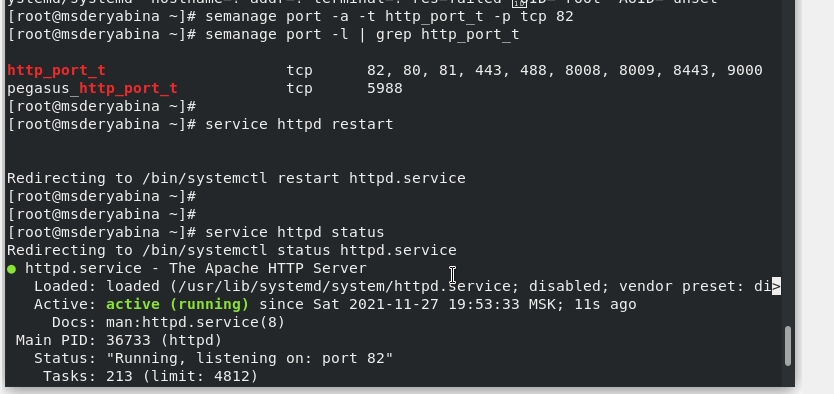


Figure 22: Добавление 82 порта и перезапуск веб-сервера

Вернула контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html и попробовала получить доступ к файлу через веб-сервер, введя в браузере http://127.0.0.1:82/test.html (рис. 23).

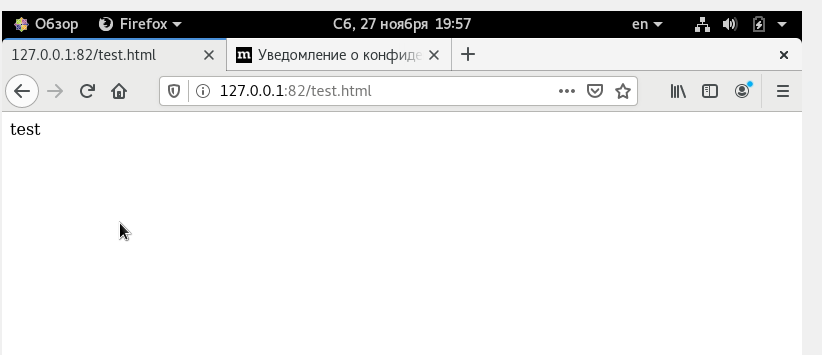


Figure 23: Доступ к файлу test.html через 82 порт

Вернула порт 80 в конфигурационный файл, удалила привязку http\_port\_t к 82 порту и удалила файл /var/www/html/test.html (рис. 24, рис. 25).

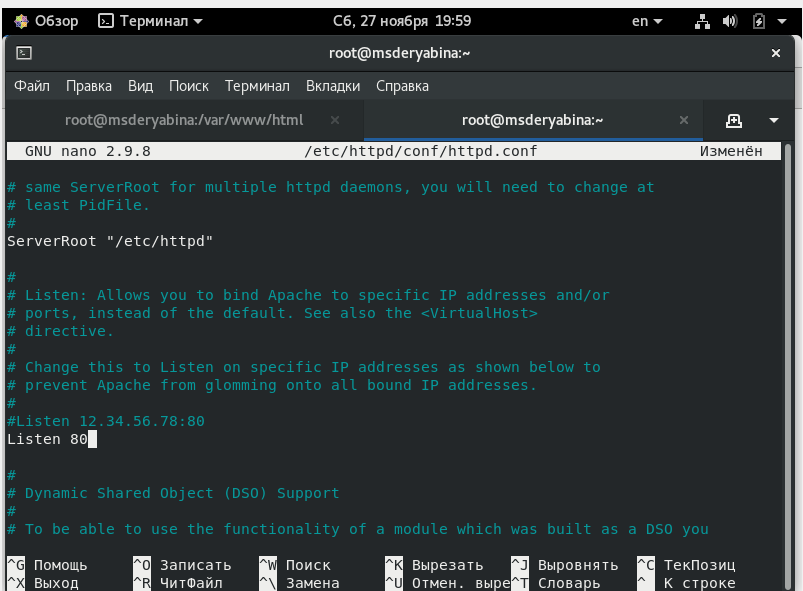


Figure 24: Восстановление исходных настроек файла httpd.conf

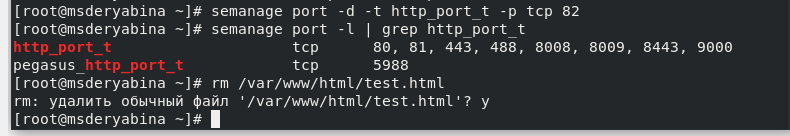


Figure 25: Восстановление исходных настроек

# Вывод

Я развила навыки администрирования ОС Linux. Получила практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.