Отчёт по лабораторной работе №6

Мандатное разгрвничение прав в Linux

Абузярова Лейла Джамилевна НБИбд-01-19

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

## 2.1 Изучение механики SetUID

Вошли в систему и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce иили sestatus.

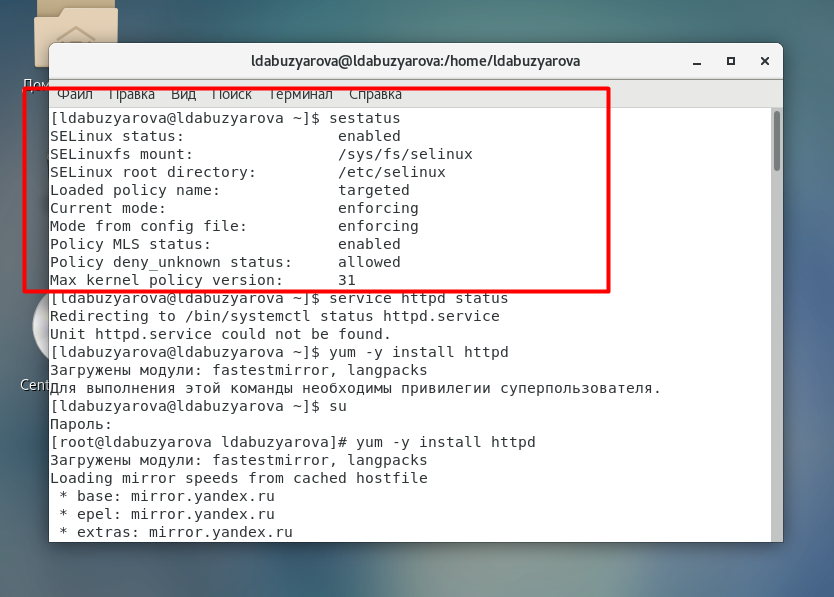


Figure 1: Подготовка к работе

Установили пакет httpd, как показано на рисунке 2.

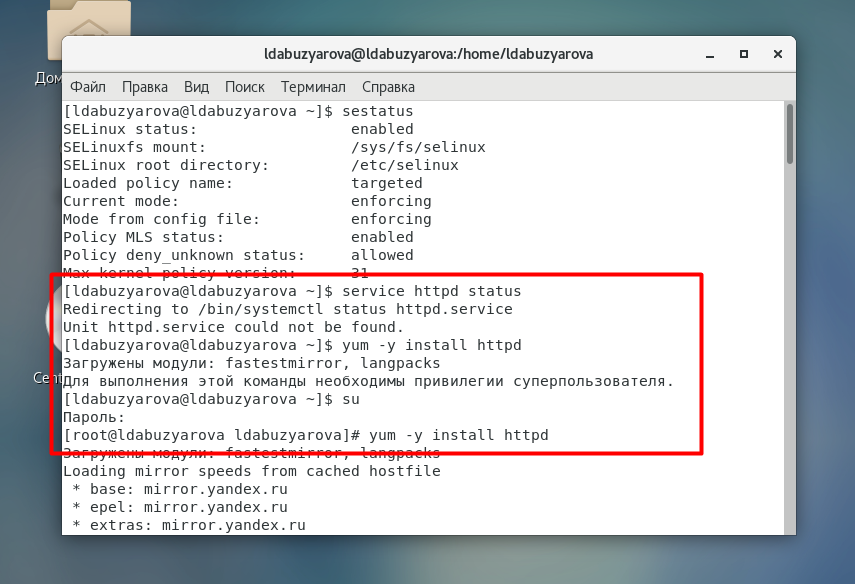


Figure 2: Установка пакета httpd

Далее с помощью команды servoce httpd status проверяем запущена ли служба, на рисунке 3 видно, что служба не запущена. В дальнейшем в ходе лабораторной работы служба будет запущена. Также найдем веб-сервер Apache в списке процессов, определим его контекст безопасности. Можно использовать команду ps auxZ | grep httpd или ps -eZ | grep httpd

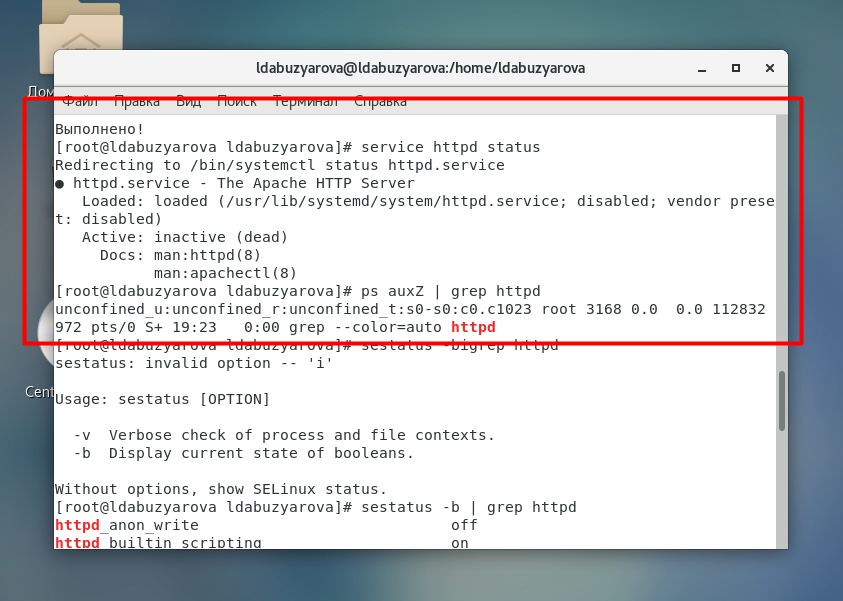


Figure 3: Проверка службы

Посмотрим текущее состояние переключателей SELinux для Apache с помощью команды sestatus -b | grep httpd Обратите внимание, что многие из них находятся в положении «off».

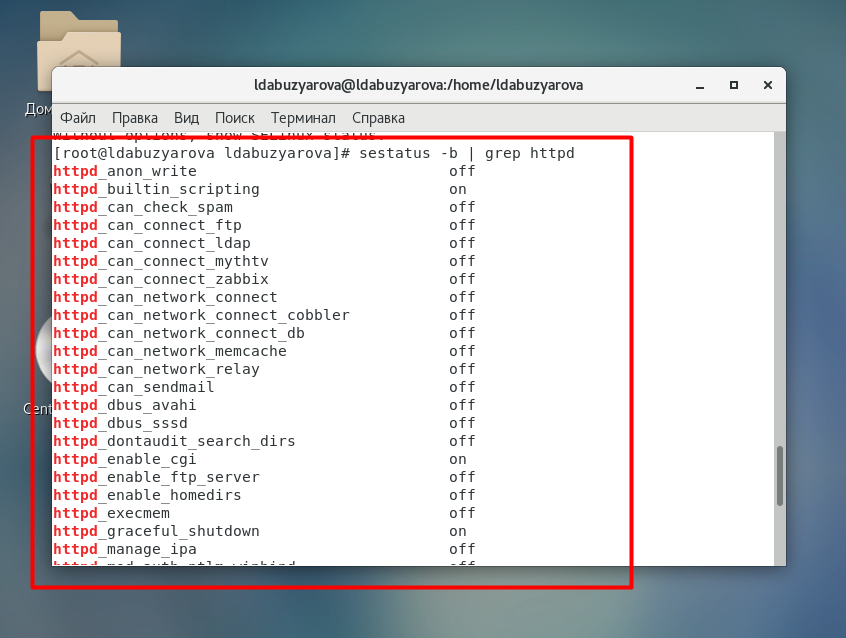


Figure 4: Переключатели SELinux для http

Посмотрим статистику по политике с помощью команды seinfo, однако в данной версии операционной системы такой команды нет. К сожалению найти аналогов команды я не смогла. Определим тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www. В поддиректориях могут располагаться системные скрипты и контент для http. Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html. В директории изначально нет файлов.

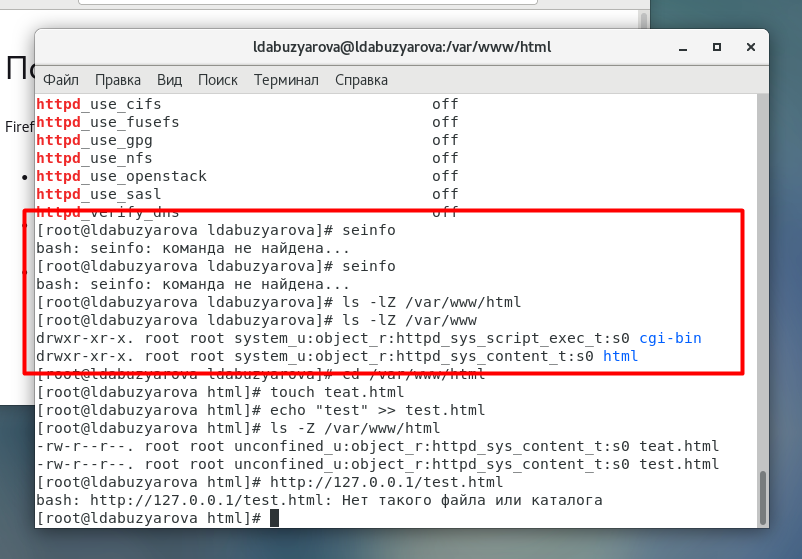


Figure 5: Определение типа файлов в директориях

Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html. Создавать файлы может только root. 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: Test. Проверим контекст созданного нами файла.

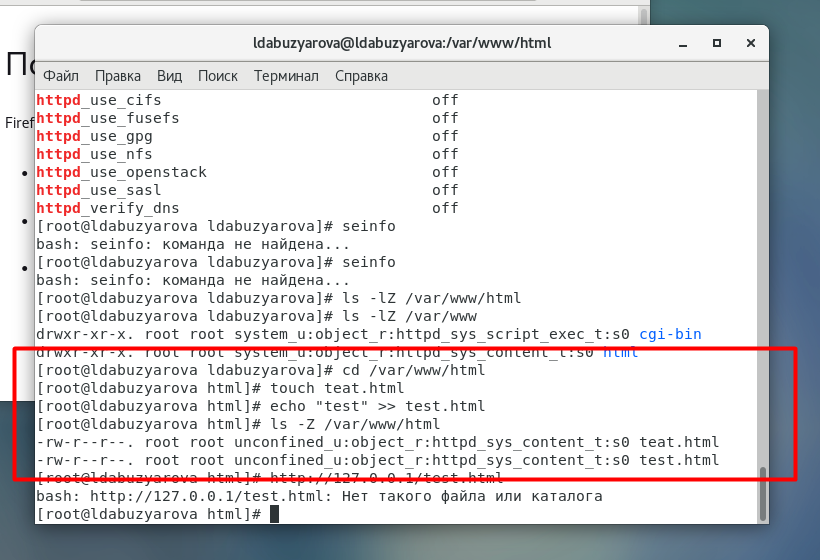


Figure 6: Создание и заполнение html-файла

Обратимся к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. К сожалению, по каким-то причинам в браузере у меня выходила ошибка, поэтому я воспользовалась консольным браузером, применяя компанду lynx. на рисунке 7 виден результат данной команды.

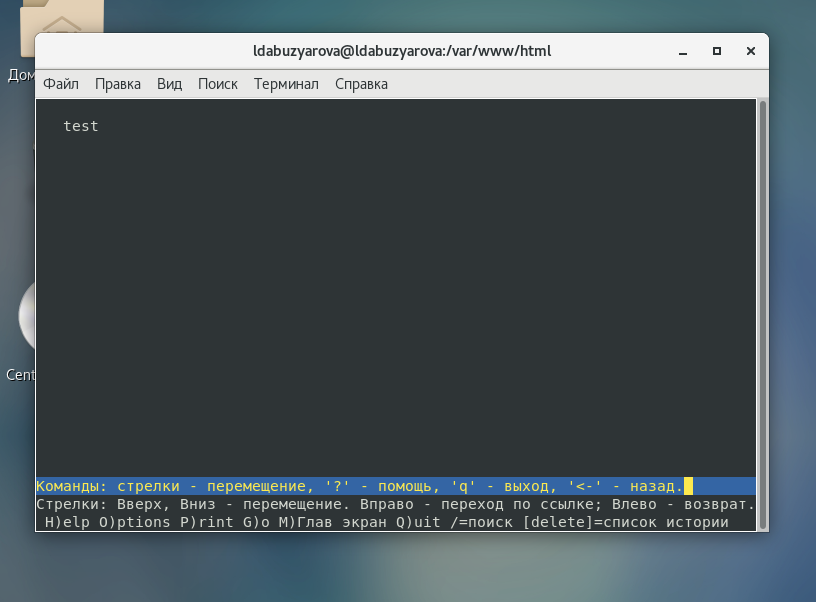


Figure 7: Проверка содержимого файла

Изучим справку man httpd\_selinux и выясним, какие контексты файлов определены для httpd. К сожалению, данная команда тоже не сработала. Далее определяем контексты типа файла test.html. Проверить контекст файла можно командой ls -Z. ls -Z /var/www/html/test.html. Основным контекстом является httpd\_sys\_content\_t, его мы и увидели в выводе команды, который изображен на рисунке 8. 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: chcon -t samba\_share\_t /var/www/html/test.html ls -Z /var/www/html/test.html После этого контекст поменялся.

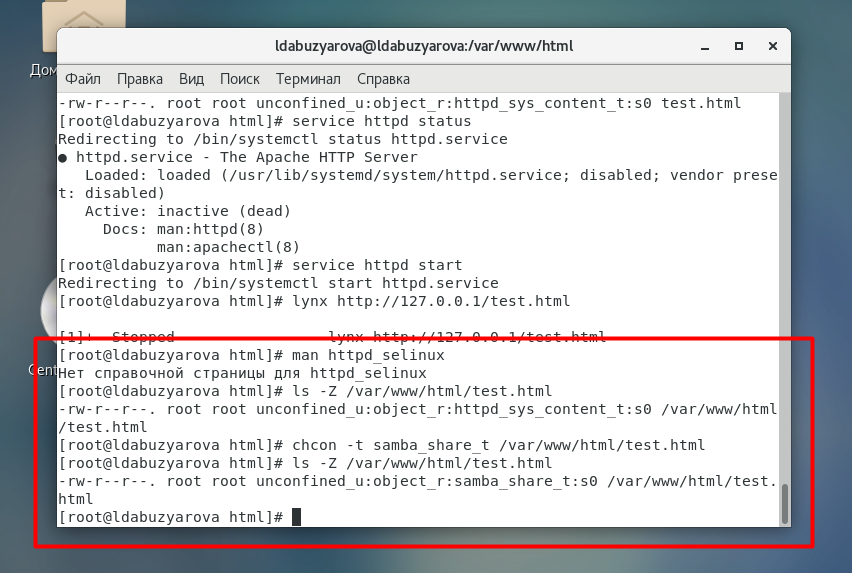


Figure 8: Проверка и изменение контекста файла

Попробуем ещё раз получить доступ к файлу через веб-сервер, в моём случае через консольный браузер. Получаем сообщение об ошибке: Forbidden You don’t have permission to access /test.html on this server. При изменении контекста файл стал считаться чужим для http и программа не может его прочитать.

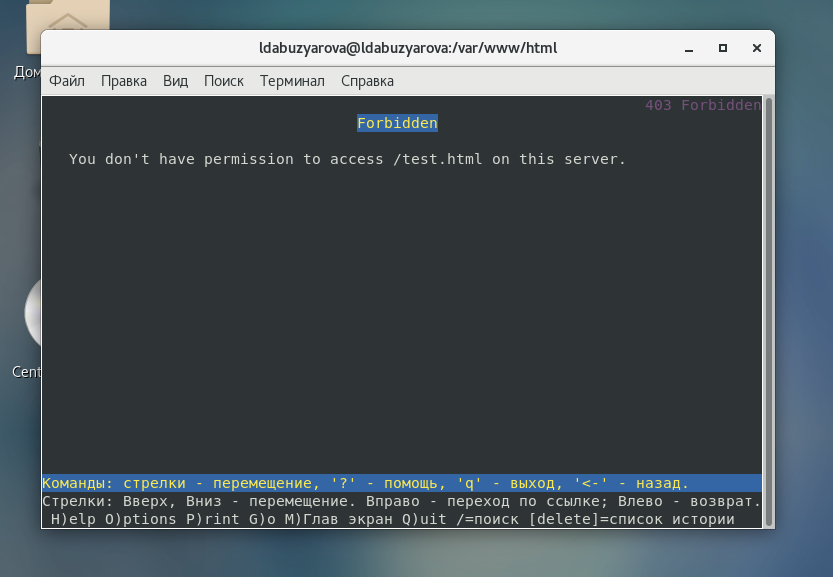


Figure 9: Ошибка доступа после изменения контекста

Проанализируем ситуацию. Согласно выводу команды ls -l /var/www/html/test.html файл на чтение доступен, но так как ранее мы сменили контекст, то в браузере выходит ошибка. Теперь просмотрим log-файлы веб-сервера Apache. Также просмотрим системный лог-файл: tail /var/log/messages.

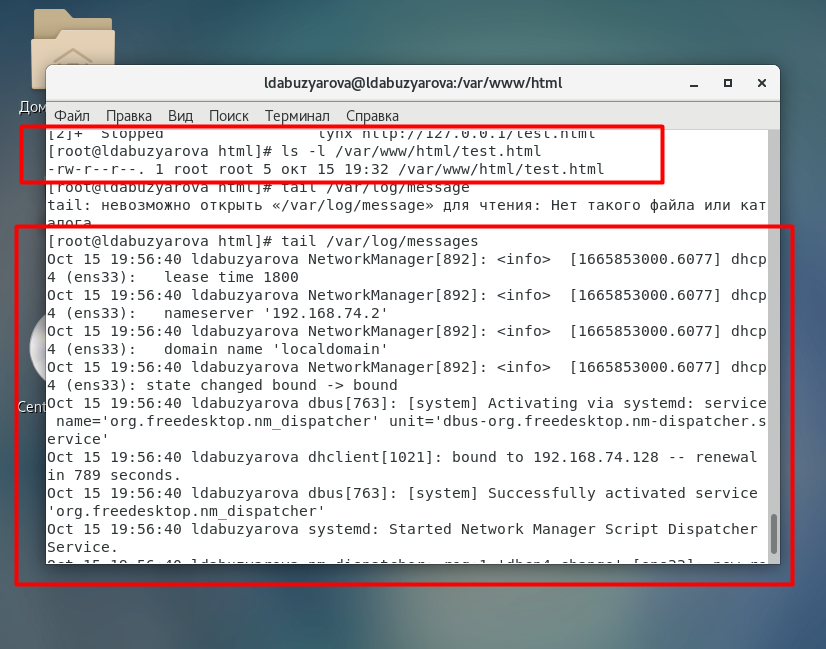


Figure 10: Лог ошибок

Если в системе окажутся запущенными процессы setroubleshootd и audtd, то мы также сможем увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log. Убеждаемся в ошибке.

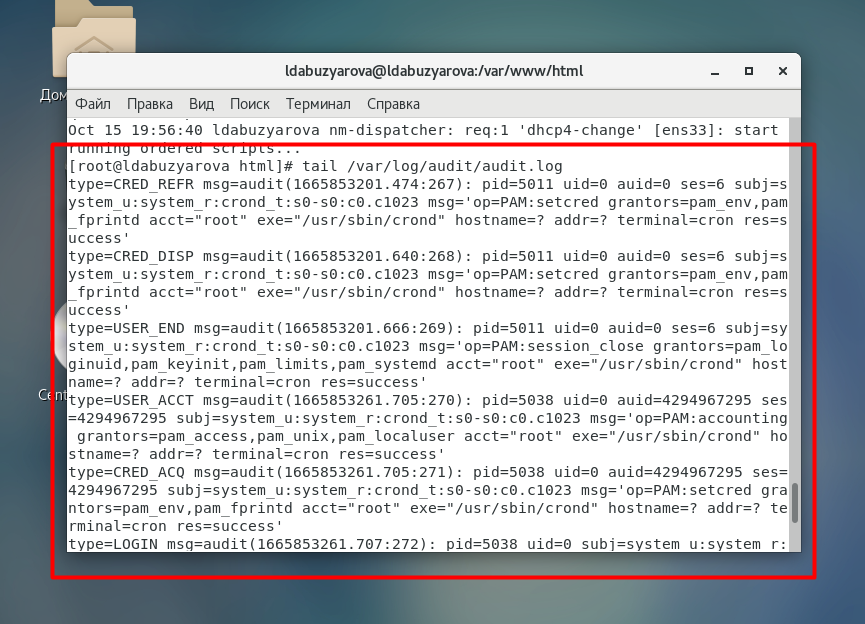


Figure 11: Лог ошибок

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 замените её на Listen 81.

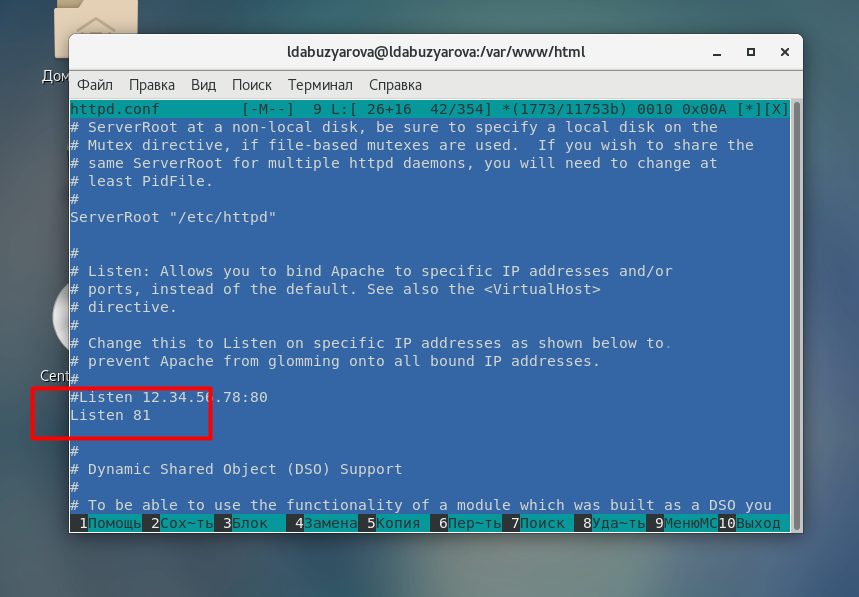


Figure 12: Переключение порта

Выполним перезапуск веб-сервера Apache. Сбой не происходит, порт 81 уже вписан в разрешенные.

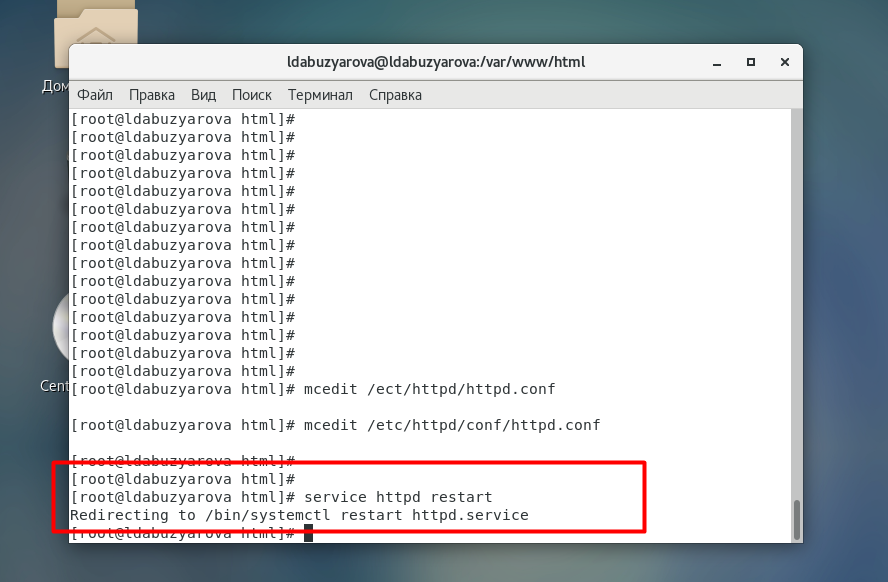


Figure 13: Проверка на сбой

Выполним 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.

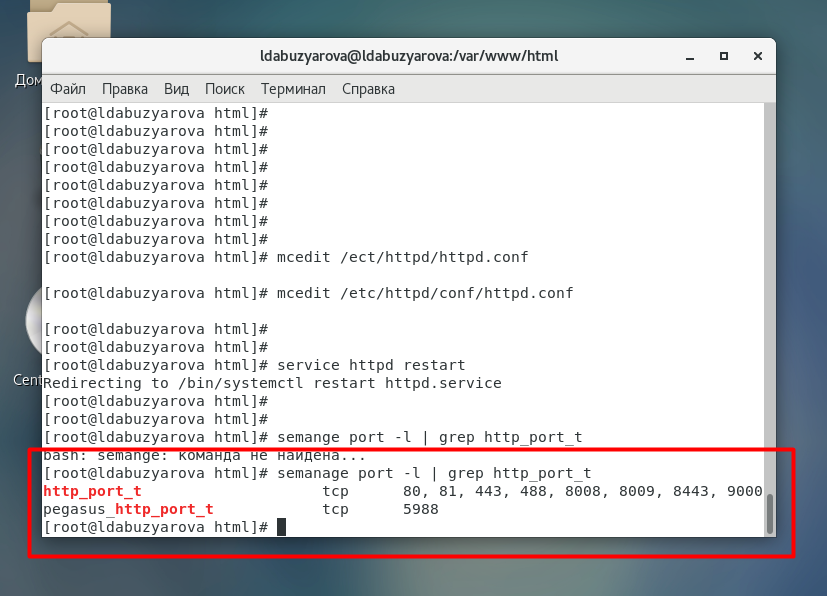


Figure 14: Проверка списка портов

Попробуем запустить веб-сервер Apache ещё раз. Все работает. Вернем 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. Мы видмть содержимое файла — слово «test», на рисунке 15.

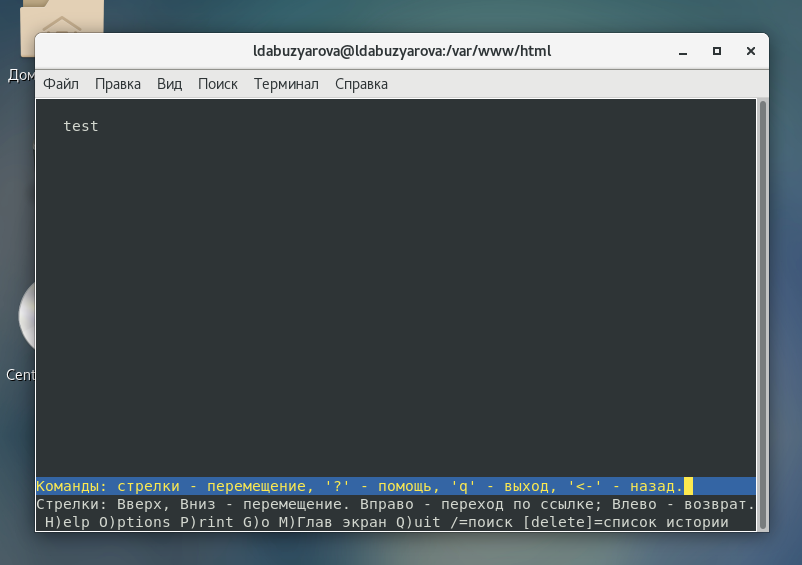


Figure 15: Содержимое файла

Исправим обратно конфигурационный файл apache, вернув Listen 80, как показано на рисунке 16.

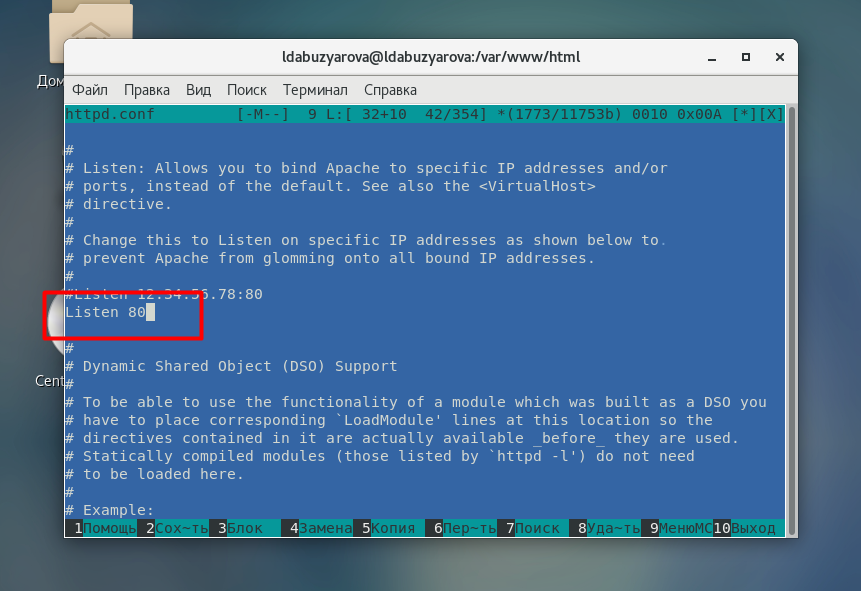


Figure 16: Повторное переключение порта

Попробуем удалить привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81. Однако, порт не может быть удален, потмоу тчо является системным и отвечает за установление связи между хостами.

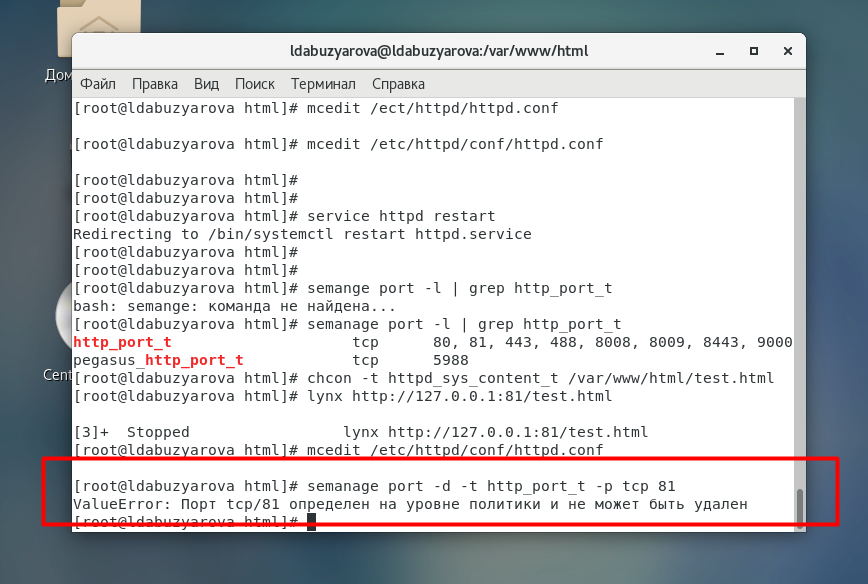


Figure 17: Неудачная попытка удалить 81 порт

Удалим файл /var/www/html/test.html: rm /var/www/html/test.html, как показано на рисунке 18.

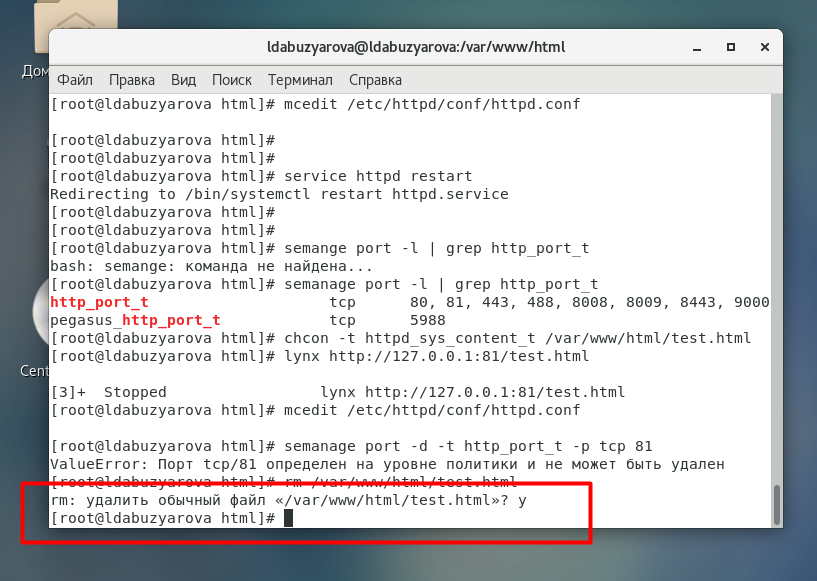


Figure 18: Удаление файла

# 3 Выводы

В процессе выполнения лабораторной работы мною были получены базовые навыки работы с технологией seLinux.

# Список литературы

1. [SELinux в CentOS](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security-enhanced_linux/index)
2. [Веб-сервер Apache](https://httpd.apache.org/)