**Отчет по лабораторной работе №6**

**Информационная безопасность**

## Нгуен Фыок Дат

**Содержание**

1. [Цель работы](#_bookmark0) 5
2. [Задание](#_bookmark1) 6
3. [Теоретическое введение](#_bookmark2) 7
4. [Выполнение лабораторной работы](#_bookmark3) 8
5. [Выводы](#_bookmark25) 16

[Список литературы](#_bookmark26) 17

**Список таблиц**

**Список иллюстраций**

[4.1 Проверка режима работы](#_bookmark4) . . . . . . . . . . . . . . . . . . . . . . . . . . 8

[4.2 Проверка работы веб-сервера](#_bookmark5) . . . . . . . . . . . . . . . . . . . . . . . . 8

[4.3 Запуск веб-сервера](#_bookmark6) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9

[4.4 Определение контекста безопасности](#_bookmark7) . . . . . . . . . . . . . . . . . . . . 9 [4.5 Просмотр переключателей](#_bookmark8) 10

* 1. [Статистика по политике](#_bookmark9) 11
  2. [Определение типов поддиректорий](#_bookmark10) 11
  3. [Создание файла test.html](#_bookmark11) 12
  4. [Проверка контекста test.html](#_bookmark12) 12
  5. [Просмотр файла в браузере](#_bookmark13) 12
  6. [Смена контекста](#_bookmark14) 12
  7. [Просмотр файла в браузере](#_bookmark15) 13
  8. [Чтение лог-файлов](#_bookmark16) 13
  9. [Смена порта](#_bookmark17) 13
  10. [Перезапуск веб-сервера](#_bookmark18) 14
  11. [Проверка лог-файлов](#_bookmark19) 14
  12. [Просмотр списка портов](#_bookmark20) 14
  13. [Смена контекста](#_bookmark21) 15
  14. [Просмотр файла](#_bookmark22) 15
  15. [Изменение порта](#_bookmark23) 15
  16. [Попытка удаления порта](#_bookmark24) 15

# Цель работы

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

# Задание

* + Поиск информации про веб-сервер
  + Работа с Html-файлами
  + Просмотр лог-файлов

# Теоретическое введение

SELinux представляет собой систему маркировки, каждый процесс файл, каталог, пользователь, устройство, порт и так далее имеет метку. SELinux определяет правила доступа процесса к объектам с определенными метками. Это называется политикой.

Владелец файла не имеет полной свободы действий над атрибутами безопасности. Стандартные атрибуты контроля доступа, такие как группа и владелец ничего не зна- чат для SELinux. Полностью все управляется метками. Значения атрибутов могут быть установлены и без прав root, но на это нужно иметь специальные полномочия SELinux.

SELinux может работать в трех режимах — отключен, система полностью отключена и не работает, режим ограничений Enforcing — программа активирована и блокирует все не соответствующие политикам действия и третий режим Permissive — только фиксировать нарушения.

Политики SELinux бывают тоже нескольких типов. Политика targeted относится к типу Type Enforcment (TE) политик, в которых управление доступом к файлам осуществляется на основе ролей. Сюда же относится политика strict. Есть ещё политики Multi-Level Security (MLS), в которых добавлены дополнительные категории.

Более подробно о см. в [1,2].

# Выполнение лабораторной работы

В качестве первого шага лабораторной работы мы проверили режим работы SELinux с помощью команд getenforce и sestatus (рис. [4.1).](#_bookmark4)

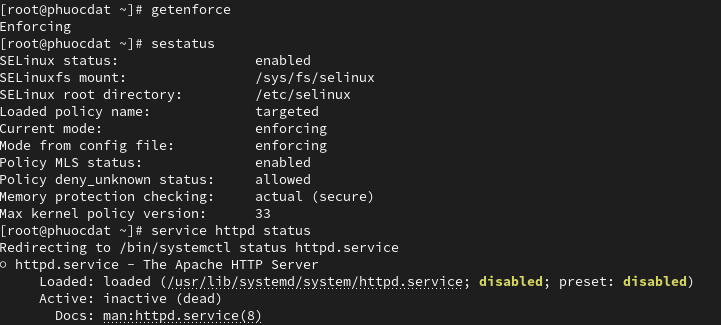
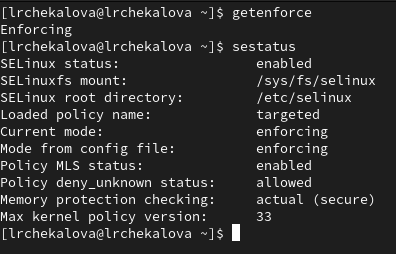


Рис. 4.1: Проверка режима работы

Далее мы проверили, работает ли веб-сервер (рис. [4.2),](#_bookmark5) и запустили его, так как он не работал (рис. [4.3).](#_bookmark6)

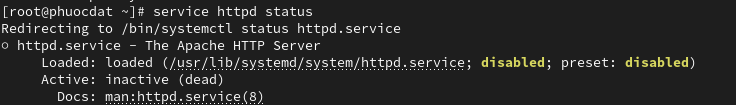
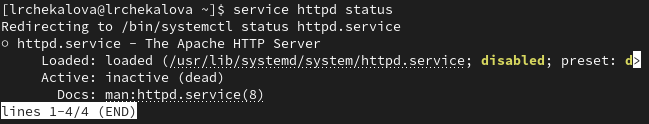


Рис. 4.2: Проверка работы веб-сервера

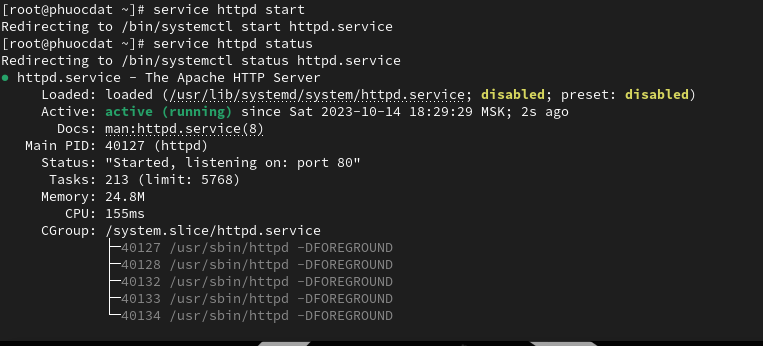
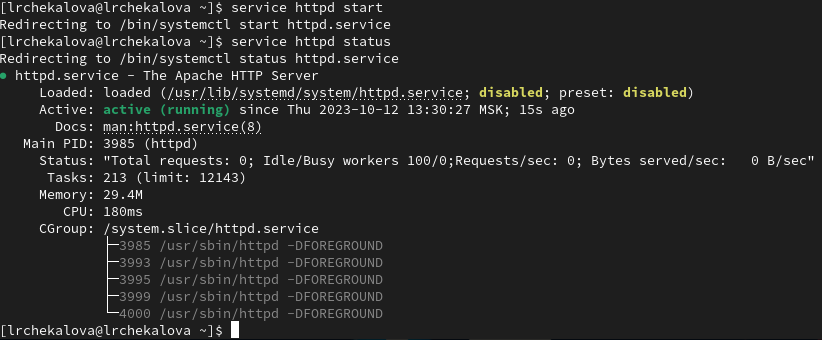


Рис. 4.3: Запуск веб-сервера

Определили контекст безопасности процесса веб-сервера (рис. [4.4).](#_bookmark7) Главной информа- цией для нас стал тип процесса — httpd\_t.

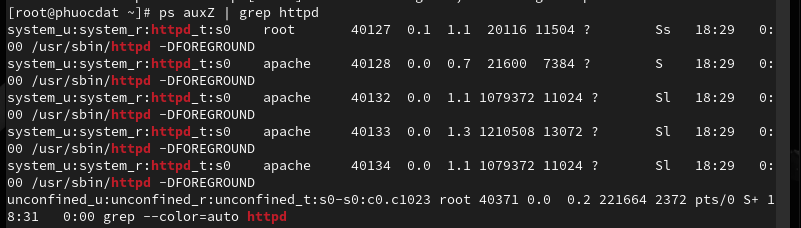
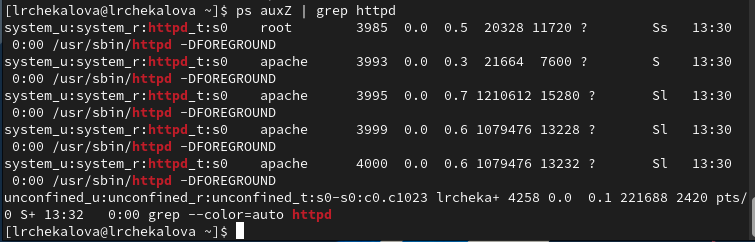


Рис. 4.4: Определение контекста безопасности

Посмотрели текущее положение переключателей SELinux, большинство из них нахо- дятся в выключенном состоянии (рис. [4.5).](#_bookmark8)

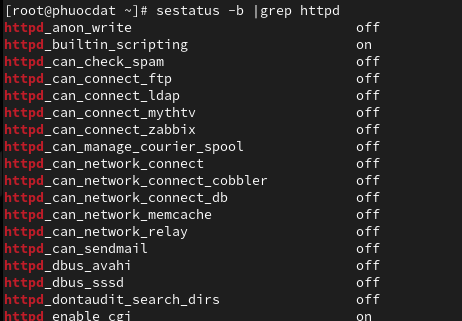
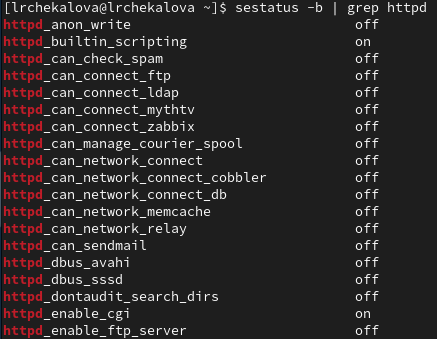


Рис. 4.5: Просмотр переключателей

Посмотрели статистику по политике с помощью seinfo (рис. [4.6).](#_bookmark9) Определили, что множество пользователей имеет размер 8, множество ролей — 14, а множество типов — 5100.

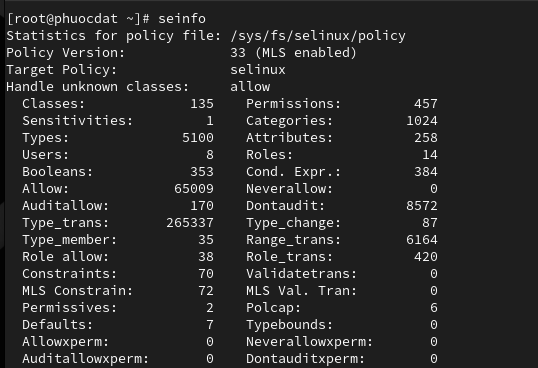
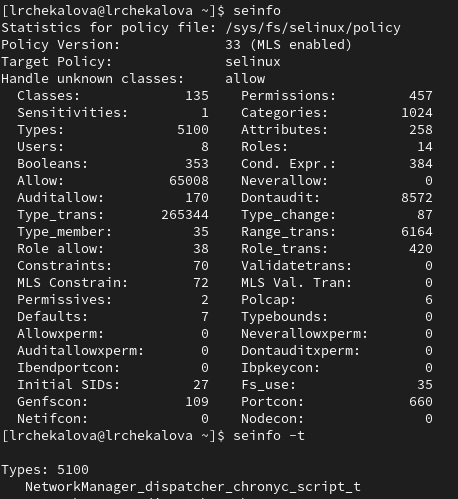


Рис. 4.6: Статистика по политике

Определили тип файлов и поддиректорий директории /var/www (рис. [4.7).](#_bookmark10) Поддирек- тория cgi-bin имеет тип httpd\_sys\_script\_exec\_t, а html — httpd\_sys\_content\_t. Только пользователь-владелец имеет право создавать файлы в папке html.

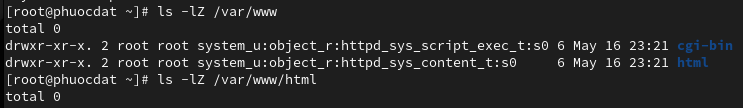
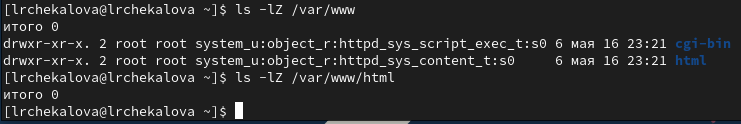


Рис. 4.7: Определение типов поддиректорий

Создали файл test.html в папке html от лица суперпользователя (рис. [4.8).](#_bookmark11)

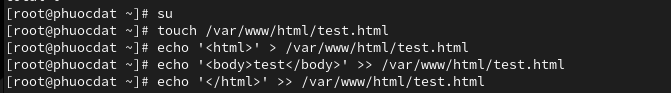
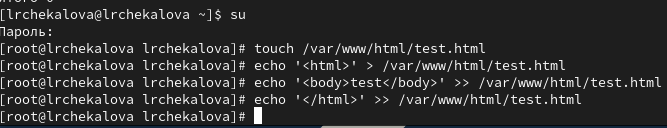


Рис. 4.8: Создание файла test.html

Проверили его контекст (рис. [4.9).](#_bookmark12) Вновь созданным файлам в папке html по умолчанию присваивается тип httpd\_sys\_content\_t.



Рис. 4.9: Проверка контекста test.html

Обратились к файлу через веб-сервер и увидели его содержимое (рис. [4.10).](#_bookmark13)

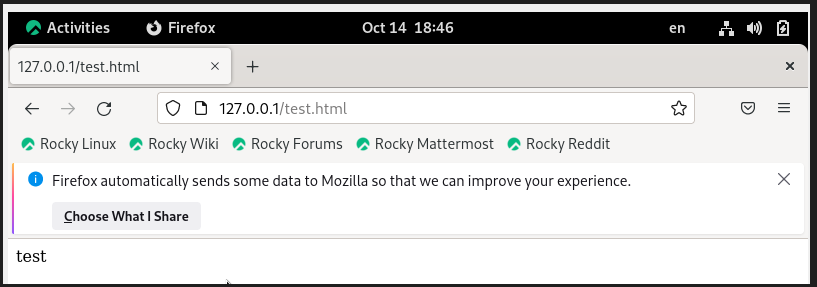
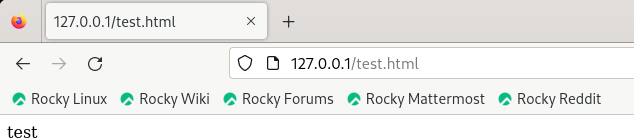


Рис. 4.10: Просмотр файла в браузере

Снова проверили контекст файла и поменяли его на другой (рис. [4.1](#_bookmark14)1). Новый контекст файла не позволяет процессу httpd получить доступ к файлу при обращении к нему через браузер.

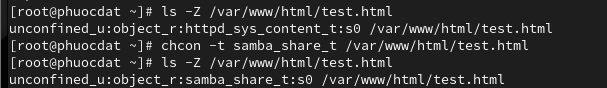
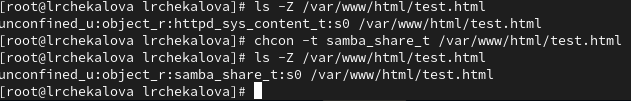


Рис. 4.11: Смена контекста

Попробовали открыть файл в браузере (рис. [4.12).](#_bookmark15) Возникла ошибка из-за нового контекста.

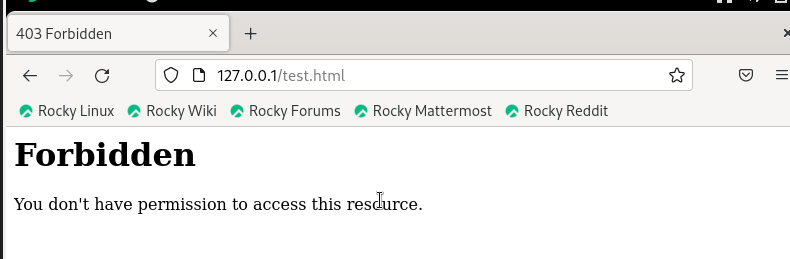
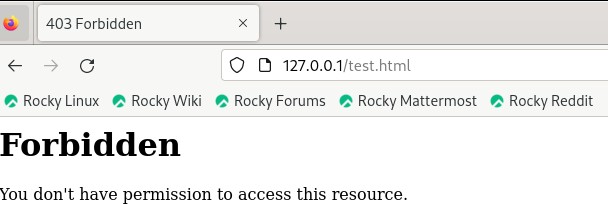


Рис. 4.12: Просмотр файла в браузере

Посмотрели лог-файлы (рис. [4.13).](#_bookmark16) Увидели запись о неудачной попытке браузера получить доступ к файлу (ошибка 403).

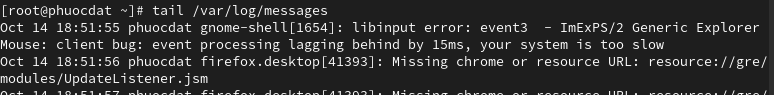
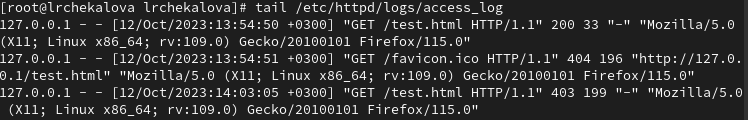


Рис. 4.13: Чтение лог-файлов

Изменили порт в конфигурационном файле httpd.conf с 80 на 81 (рис. [4.14).](#_bookmark17)

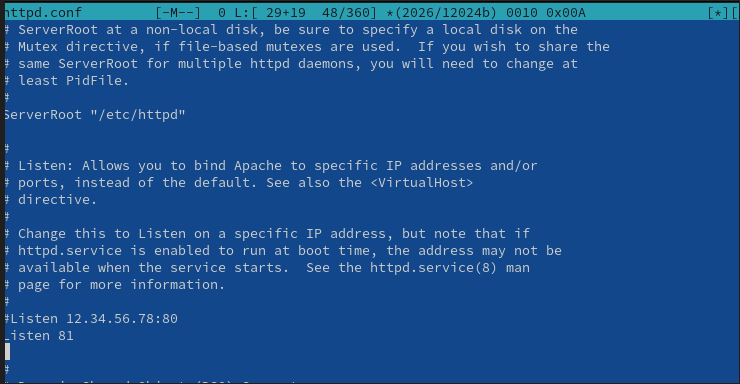
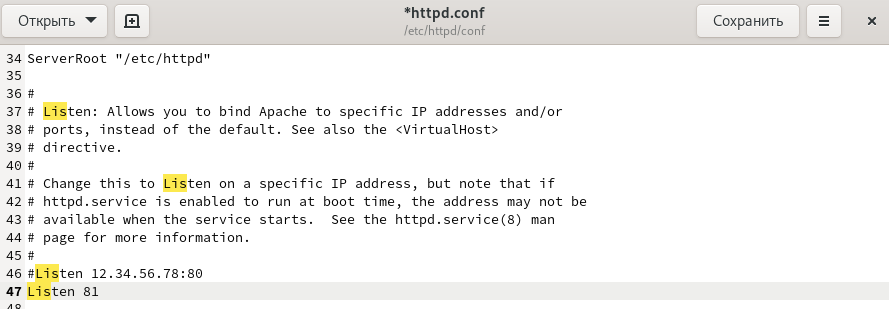
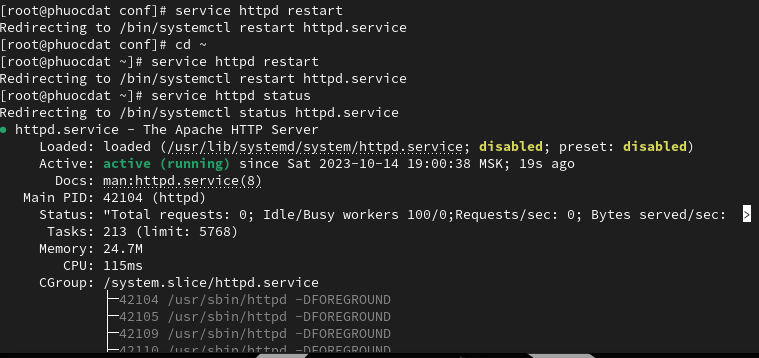
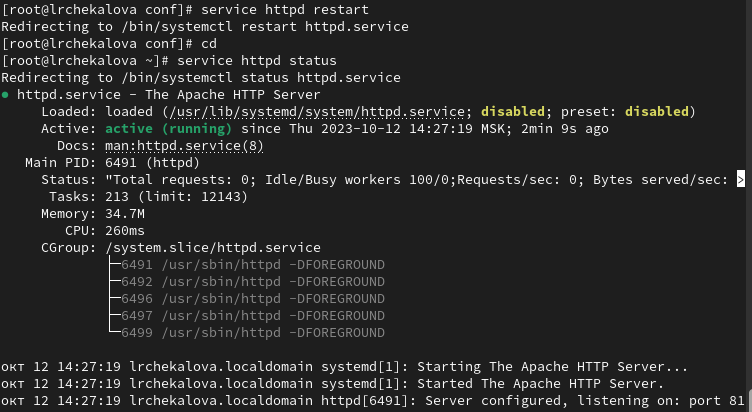


Рис. 4.14: Смена порта

Перезапустили веб-сервер, получили сообщение о том, что он запущен на прослуши- вание 81 порта (рис. [4.15).](#_bookmark18)

Рис. 4.15: Перезапуск веб-сервера



Проверили лог-файлы и нашли информацию о переключении веб-сервера на прослу- шивание нового порта (рис. [4.16).](#_bookmark19)

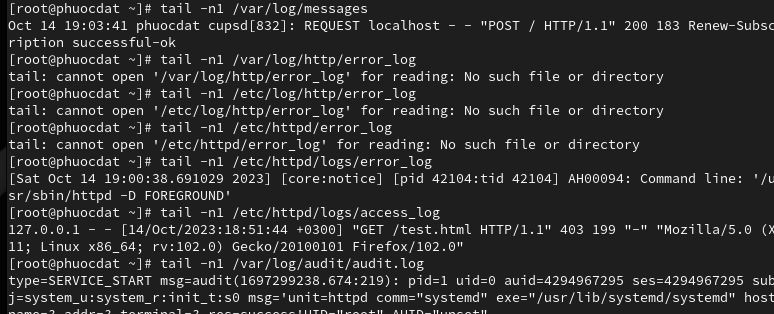
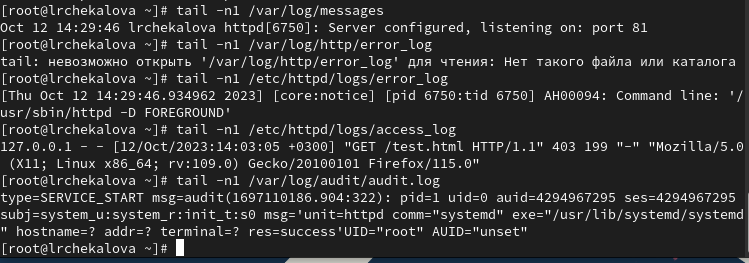


Рис. 4.16: Проверка лог-файлов

Посмотрели список портов веб-сервера, нашли там указанный нами порт (рис. [4.17).](#_bookmark20)

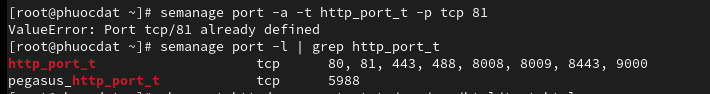
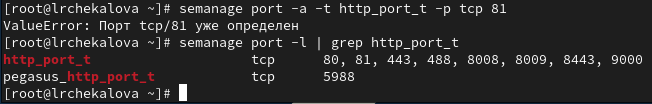


Рис. 4.17: Просмотр списка портов

Вернули файлу test.html старый контекст (рис. [4.18).](#_bookmark21)

Рис. 4.18: Смена контекста



Получили доступ к файлу через веб-сервер в браузере (рис. [4.19).](#_bookmark22)

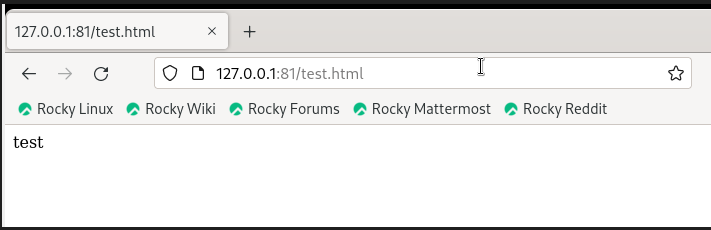
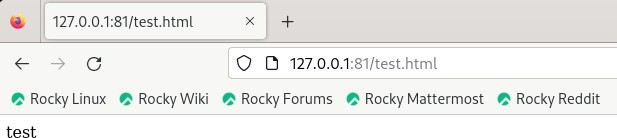


Рис. 4.19: Просмотр файла

Вернули порт 80 в конфигурационном файле (рис. [4.20).](#_bookmark23)

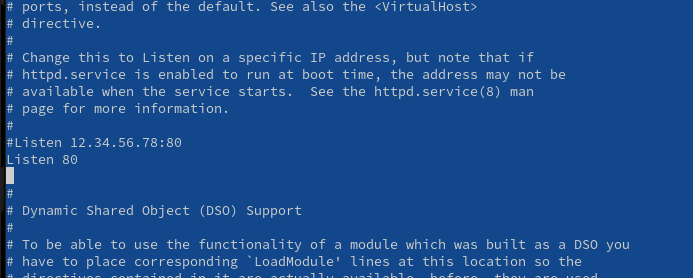
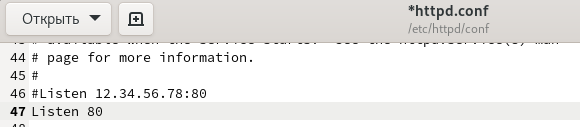


Рис. 4.20: Изменение порта

Попытались удалить 81 порт, но столкнулись с ошибкой, что он определен на уровне политики и не может быть удален (рис. [4.21).](#_bookmark24) После этого удалили файл test.html.

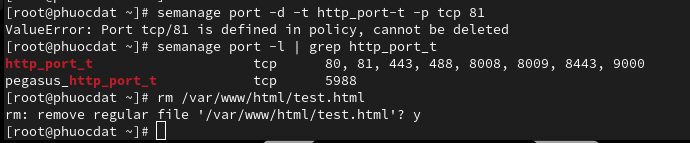
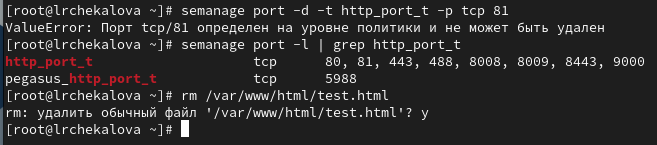


Рис. 4.21: Попытка удаления порта

# Выводы

В результате лабораторной работы я получила базовые навыки администрирования ОС Linux, познакомилась с технологией SELinux и проверила ее работу на практике совместно с веб-сервером Apache.

# Список литературы

1. Мандатное разграничение прав в Linux [Электронный ресурс]. URL: [https://esyste](https://esystem.rudn.ru/pluginfile.php/2090282/mod_resource/content/2/006-lab_selinux.pdf) [m.rudn.ru/pluginfile.php/2090282/mod\_resource/content/2/006-lab\_selinux.pdf.](https://esystem.rudn.ru/pluginfile.php/2090282/mod_resource/content/2/006-lab_selinux.pdf)
2. Настройка SELinux [Электронный ресурс]. URL: [https://losst.pro/nastrojka-selinux.](https://losst.pro/nastrojka-selinux)