Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Тимур Дмитриевич Калинин

Содержание

# 1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

# 2 Выполнение лабораторной работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus ([Рис. 1](#fig:001))

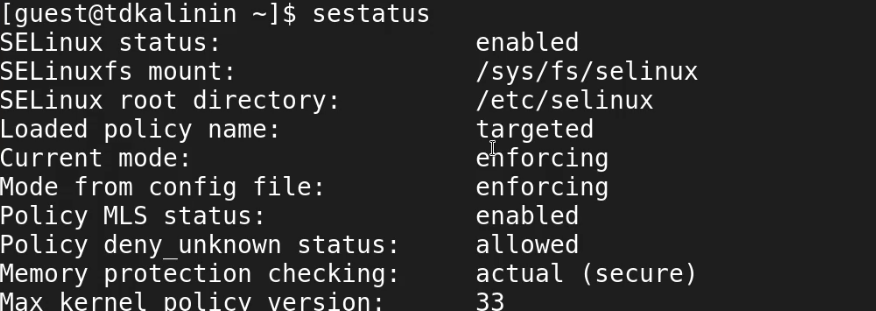


Figure 1: Статус selinux

1. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает ([Рис. 2](#fig:002)). Если не работает, запустите его так же, но с параметром start ([Рис. 3](#fig:003))

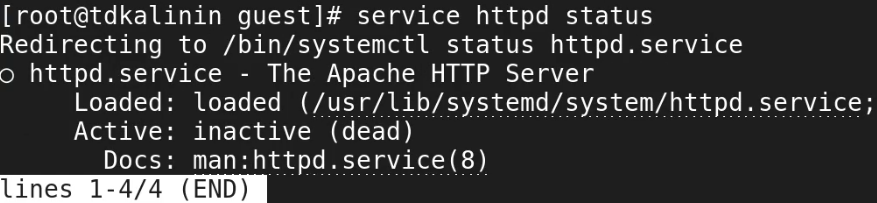


Figure 2: Статус веб-сервера

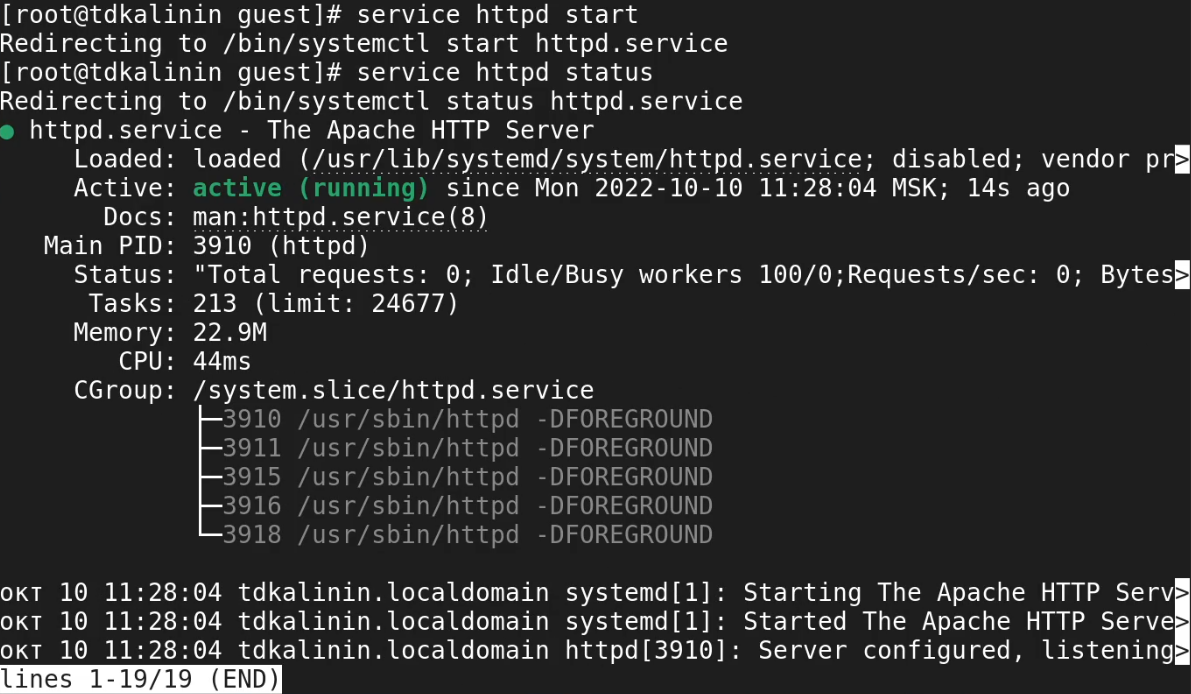


Figure 3: Запуск веб-сервера

1. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт ([Рис. 4](#fig:004)).

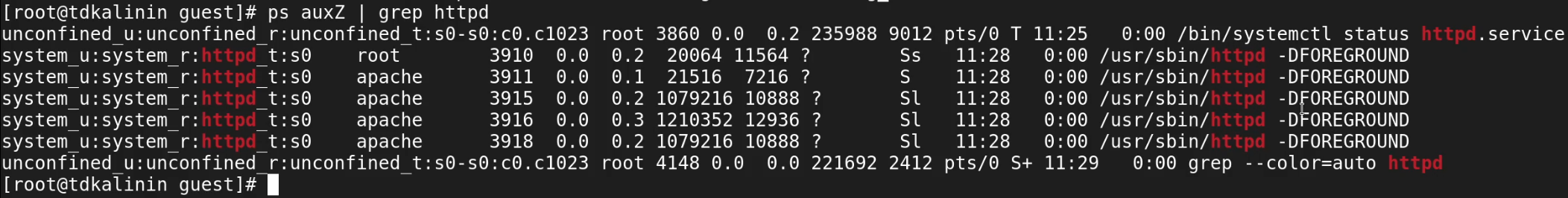


Figure 4: Контекст службы Apache

1. Посмотрите текущее состояние переключателей SELinux для Apache. Обратите внимание, что многие из них находятся в положении «off» ([Рис. 5](#fig:005)).

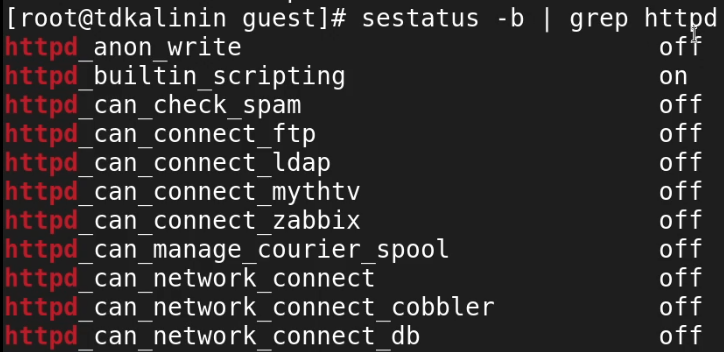


Figure 5: Состояние переключателей SELinux для Apache

1. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов ([Рис. 6](#fig:006)).

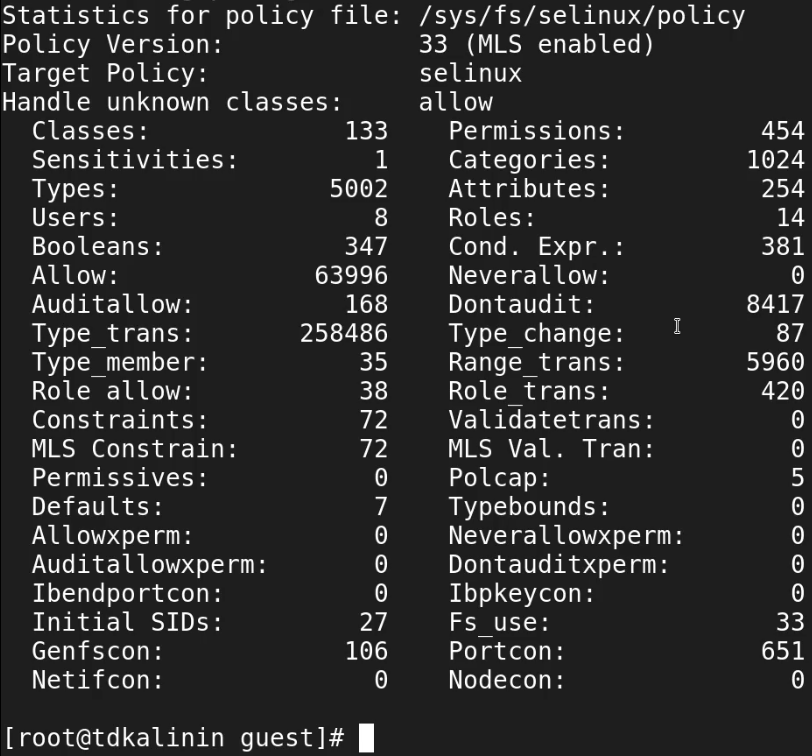


Figure 6: Статистика по политике

1. Определите тип файлов и поддиректорий, находящихся в директории /var/www ([Рис. 7](#fig:007)):

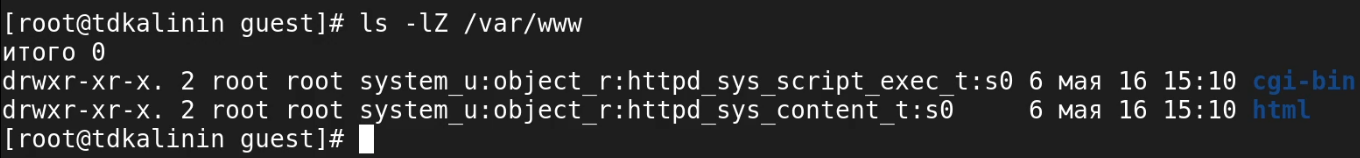


Figure 7: Тип файлов и директорий в /var/www

1. Определите тип файлов, находящихся в директории /var/www/html ([Рис. 8](#fig:008)):

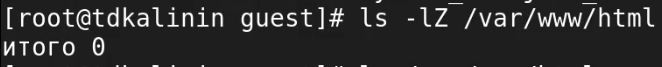


Figure 8: Тип файлов в /var/www/html

1. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html. Как видим, создание файлов разрешено только владельцу каталога.
2. Создайте 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. 9](#fig:009)):

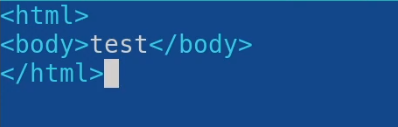


Figure 9: Содержание test.html

1. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html ([Рис. 10](#fig:010)).

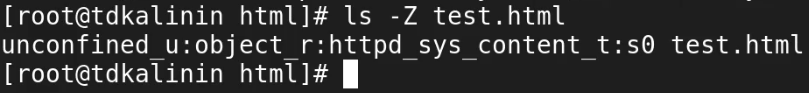


Figure 10: Контекст test.html

1. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён ([Рис. 11](#fig:011)).

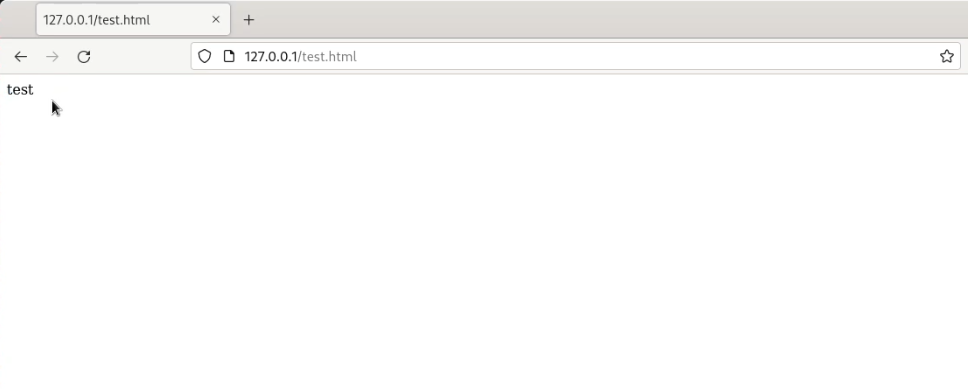


Figure 11: Обращение к файлу через веб-сервер

1. Изучите справку man httpd\_selinux и выясните, какие контексты файлов определены для httpd ([Рис. 12](#fig:012)). Сопоставьте их с типом файла test.html. Проверить контекст файла можно командой ls -Z ([Рис. 13](#fig:013)).



Figure 12: Обращение к файлу через веб-сервер

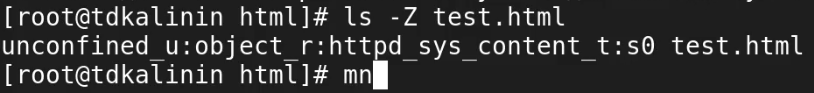


Figure 13: Контекст файла

1. Измените 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. После этого проверьте, что контекст поменялся ([Рис. 14](#fig:014)).

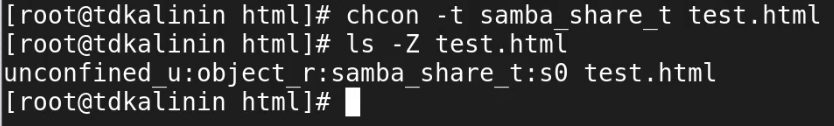


Figure 14: Изменение контекста

1. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html . Вы должны получить сообщение об ошибке ([Рис. 15](#fig:015)):

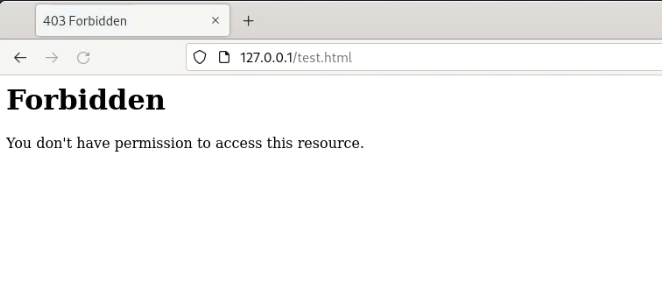


Figure 15: Проверка доступа через веб-сервер

1. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? Потому что у процесса, который пытается запросить доступ к файлу, нет к нему доступа из-за метки.

Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл ([Рис. 16](#fig:016)):

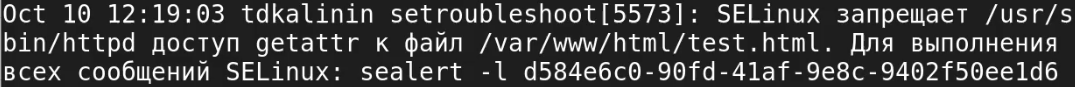


Figure 16: Системный лог-файл

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. Проверьте это утверждение самостоятельно ([Рис. 17](#fig:017)).

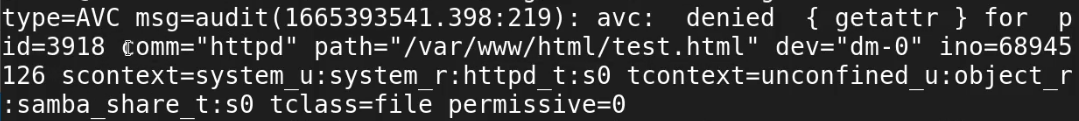


Figure 17: Файл /var/log/audit/audit.log

1. Попробуйте запустить веб-сервер Apache на прослушивание ТСР-порта 100 (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 100 ([Рис. 18](#fig:018)).

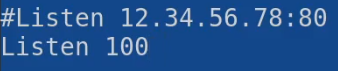


Figure 18: Прослушивание 100 порта

1. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? Сбой произошел из-за того, что у процесса нет доступа к 100 порту протокола TCP, так как он ограничивается selinux ([Рис. 19](#fig:019)).

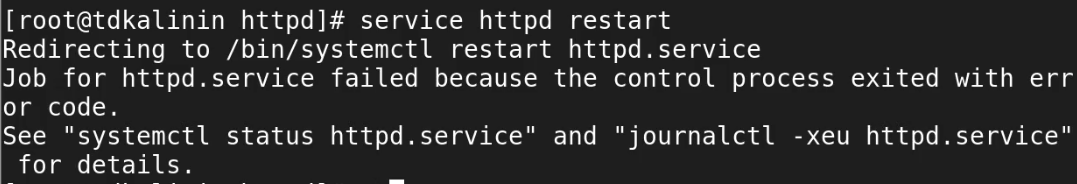


Figure 19: Сбой перезапуска

1. Проанализируйте лог-файлы ([Рис. 20](#fig:020)):

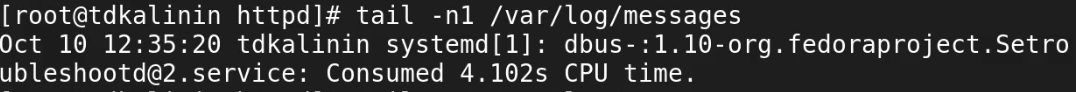


Figure 20: Содержимое системного лог-файла

Просмотрите файлы /var/log/http/error\_log ([Рис. 21](#fig:021)), /var/log/http/access\_log ([Рис. 22](#fig:022)) и /var/log/audit/audit.log ([Рис. 23](#fig:023)) и выясните, в каких файлах появились записи.

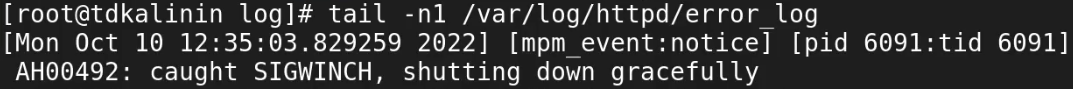


Figure 21: Содержимое /var/log/http/error\_log

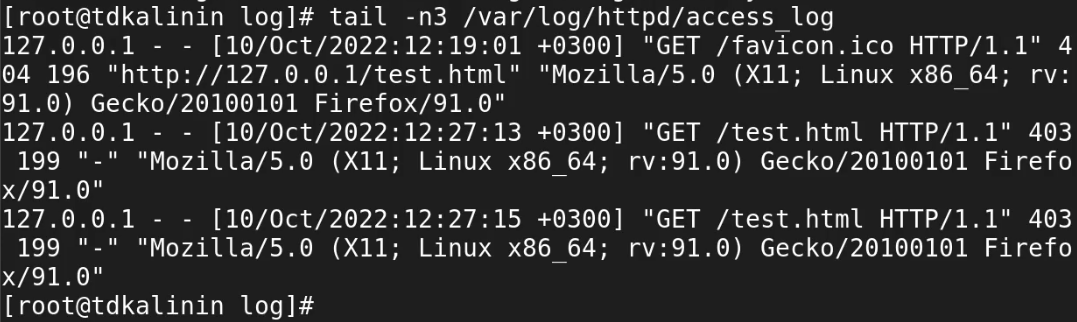


Figure 22: Содержимое /var/log/http/access\_log

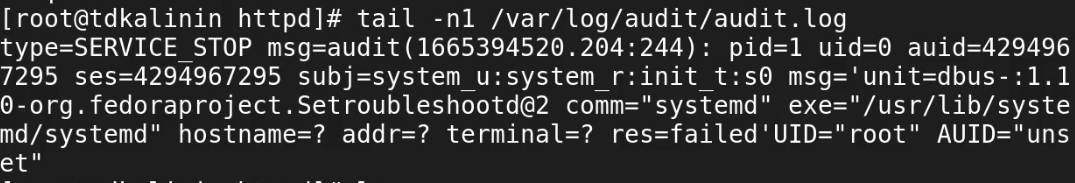


Figure 23: Содержимое /var/log/audit/audit.log

1. Выполните команду semanage port -a -t http\_port\_t -р tcp 81 После этого проверьте список портов ([Рис. 24](#fig:024))

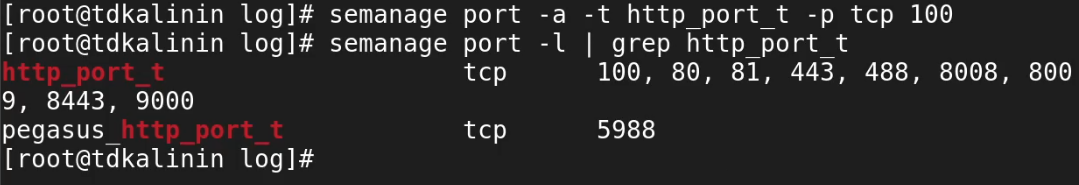


Figure 24: Добавление порта 100 для httpd

Убедитесь, что порт 100 появился в списке.

1. Попробуйте запустить веб-сервер Apache ещё раз ([Рис. 25](#fig:025)). Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог? Потому что в этот раз у процесса веб-сервера был доступ к порту 100.

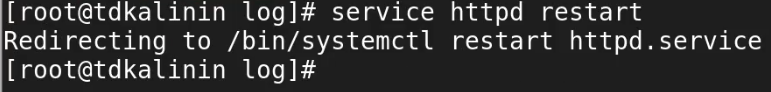


Figure 25: Перезапуск Apache

1. Верните контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html ([Рис. 26](#fig:026)):

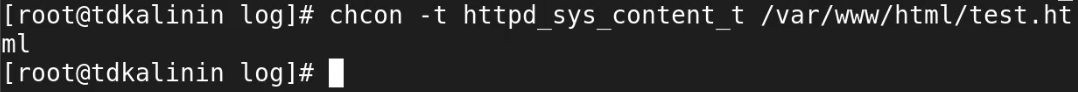


Figure 26: Возвращение контекста

После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Вы должны увидеть содержимое файла — слово «test» ([Рис. 27](#fig:027)).

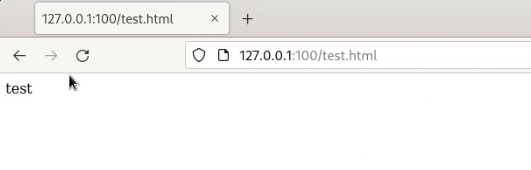


Figure 27: Доступ через браузер

1. Исправьте обратно конфигурационный файл apache, вернув Listen 80 ([Рис. 28](#fig:028)).

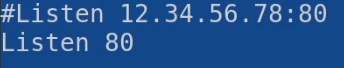


Figure 28: Исправление конфигурационного файла

1. Удалите привязку http\_port\_t к 100 порту и проверьте, что порт 100 удалён ([Рис. 29](#fig:029)).



Figure 29: Удаление 100 порта

1. Удалите файл /var/www/html/test.html ([Рис. 30](#fig:030)):

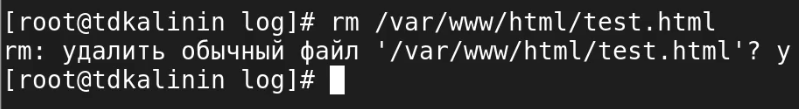


Figure 30: Удаление test.html

# 3 Выводы

Мы развили навыки администрирования ОС Linux и получили первое практическое знакомство с технологией SELinux. Проверили работу SELinx на практике совместно с веб-сервером Apache.

# 4 Библиография

1. Лабораторная работа №6. - 5 с. URL: <https://esystem.rudn.ru/pluginfile.php/1651891/mod_resource/content/2/006-lab_selinux.pdf>