Отчет по лабораторной работе №6

Информационная безопасноть

Астафьева Анна Андреевна НПИбд-01-18

Содержание

# Цель работы

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

# Теоретическое описание

SELinux — набор технологий расширения системы безопасности Linux. Сегодня основу набора составляют три технологии: мандатный контроль доступа, ролевой доступ RBAC и система типов (доменов). Apache – это свободное программное обеспечение для размещения веб-сервера. Он хорошо показывает себя в работе с масштабными проектами, поэтому заслуженно считается одним из самых популярных веб-серверов. Кроме того, Apache очень гибок в плане настройки, что даёт возможность реализовать все особенности размещаемого веб-ресурса.

# Подготовка лабораторного стенда:

1. В конфигурационном файле /etc/httpd/httpd.conf задала параметр ServerName. (рис. 1).

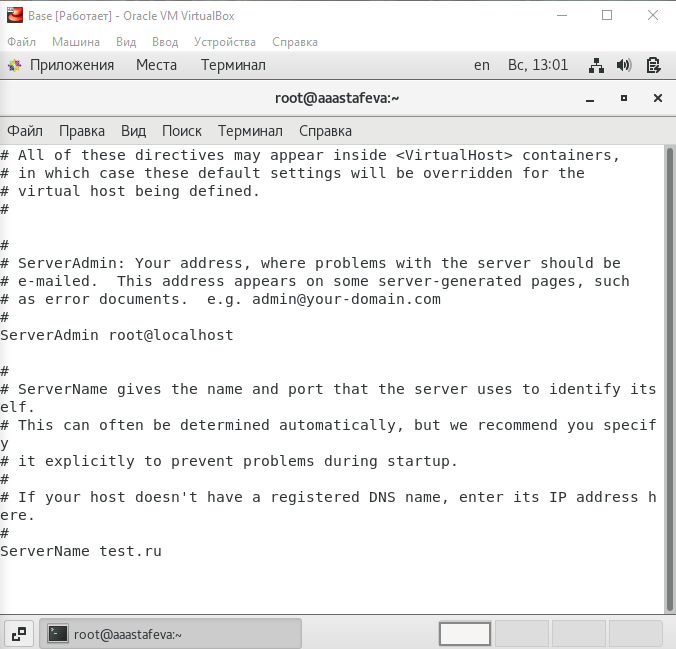


Figure 1: Параметр ServerName

1. Также проследила, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключила фильтр командами: iptables -F, iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT. Так же добавила разрешающие правила. (рис. 2), (рис. 3).

Figure 2: Отключение фильтра

Figure 2: Отключение фильтра

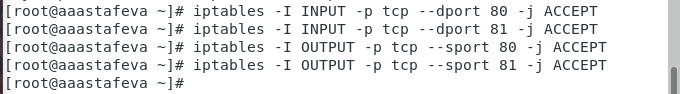


Figure 3: Добавление разрешающих правил

# Выполнение лабораторной работы

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

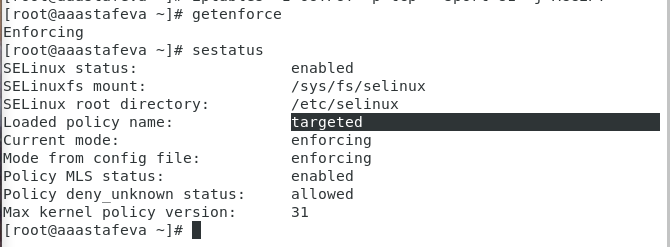


Figure 4: Проверка

1. Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает: service httpd status(рис. 5), (рис. 6).

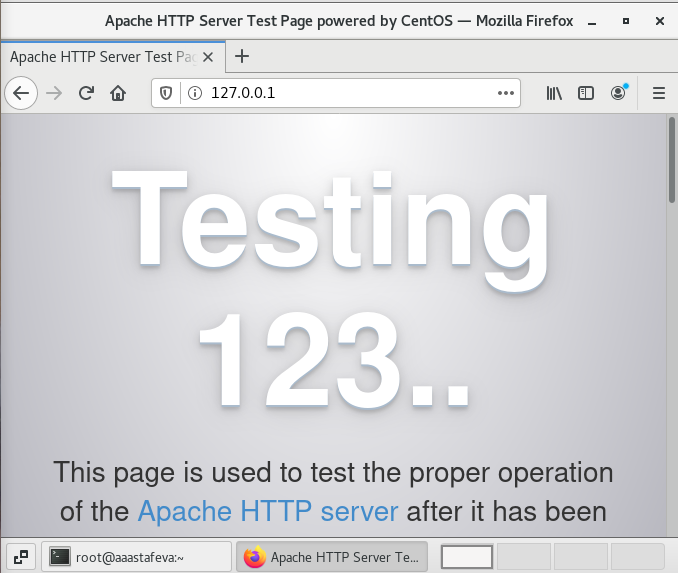


Figure 5: Обращение через браузер

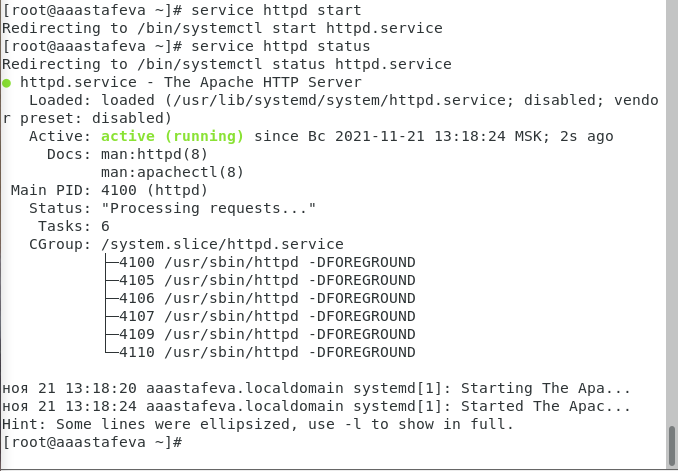


Figure 6: Проверка

1. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности (рис. 7).

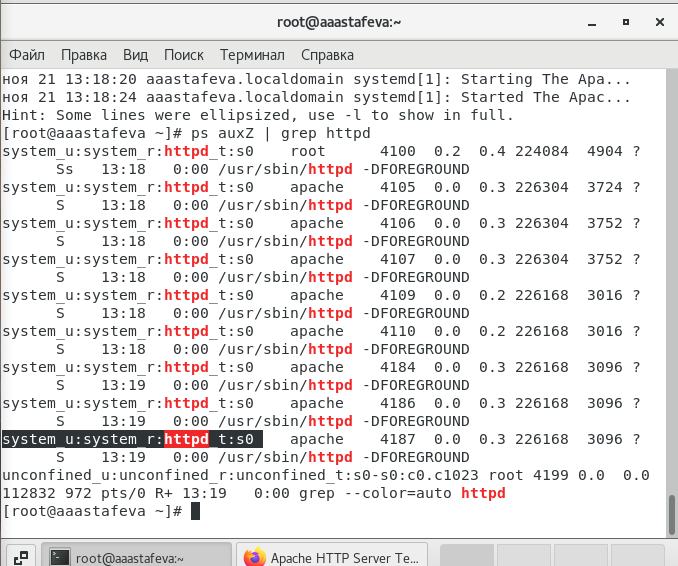


Figure 7: веб-сервер Apache

1. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды: sestatus -bigrep httpd. Обратила внимание, что многие из них находятся в положении «off». (рис. 8).

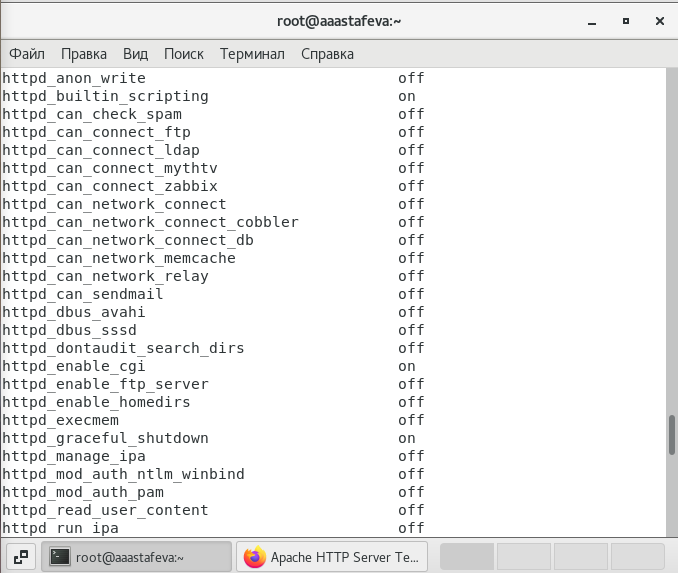


Figure 8: Просмотр состояние переключателей SELinux для Apache

1. Посмотрела статистику по политике с помощью команды seinfo, также определила множество пользователей(8), ролей(14), типов(4793). Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды: ls -lZ /var/www. Определила тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html. (рис. 9), (рис. 10).

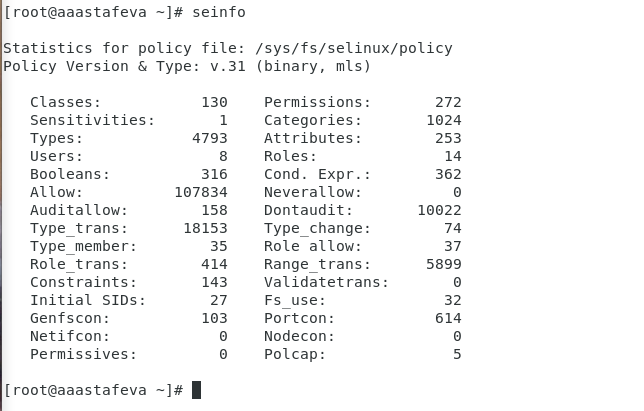


Figure 9: Получение информации

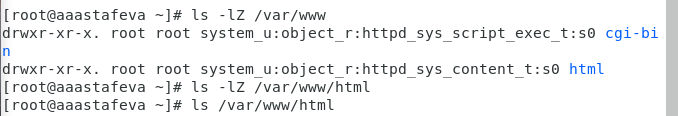


Figure 10: Получение информации

1. Создала от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html(рис. 11).

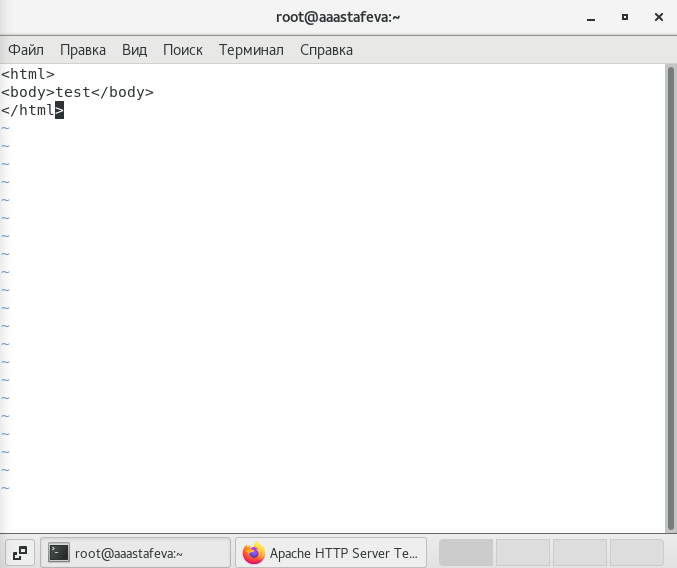


Figure 11: Создание файла

1. Проверила контекст созданного файла. httpd\_sys\_content\_t (рис. 12).

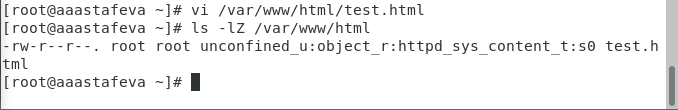


Figure 12: Проверка

1. Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедилась, что файл был успешно отображён. (рис. 13).

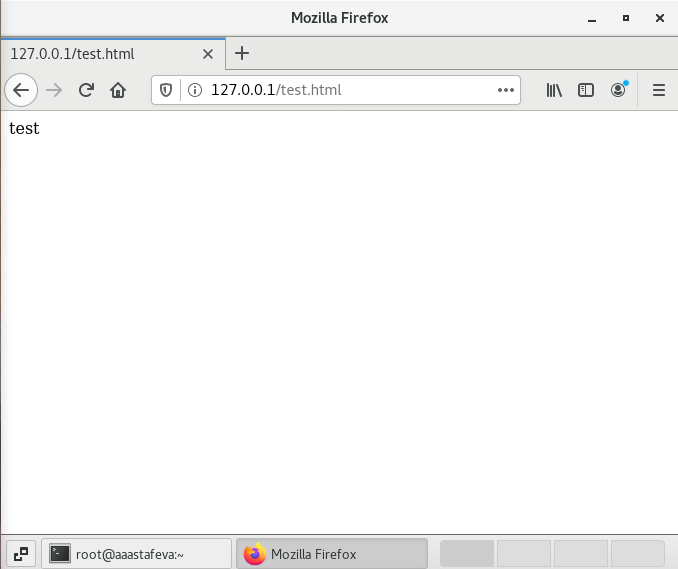


Figure 13: Получение доступа к файлу через браузер

1. Изменила контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t. После этого проверила, что контекст поменялся. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получили сообщение об ошибке. (рис. 14).

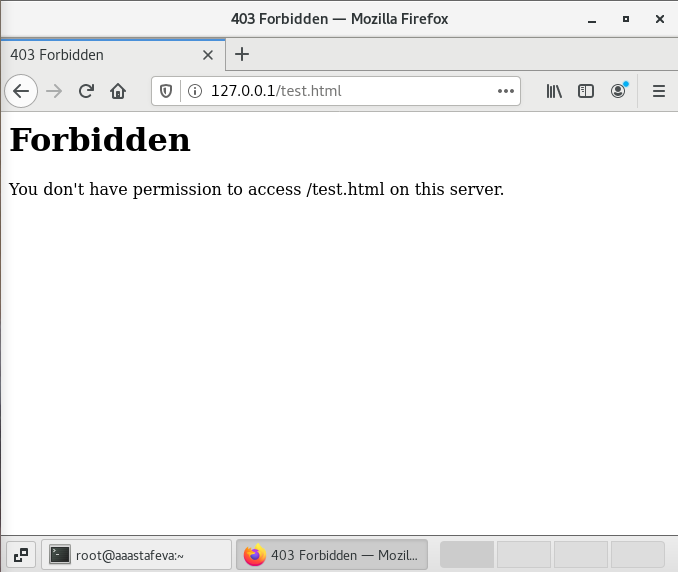


Figure 14: Получение доступа к файлу через браузер

1. Проанализировала ситуацию. Файл не был отображён потому что мы изменили контекст файла. Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл: tail /var/log/messages (рис. 15), (рис. 16).

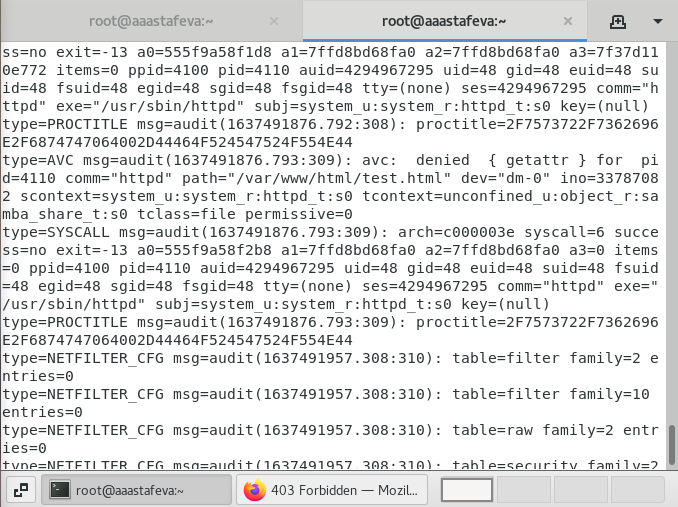


Figure 15: Просмотр системного лог-файла

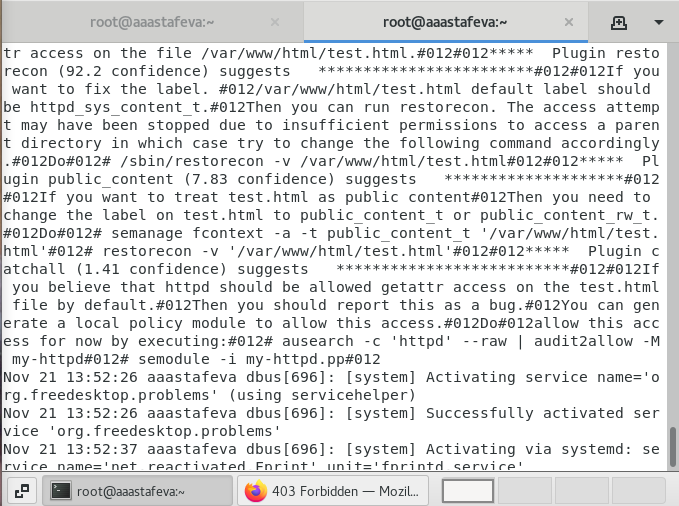


Figure 16: Просмотр системного лог-файла

1. Попробовала 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 нашла строчку Listen 80 и замените её на Listen 81.(рис. 17).

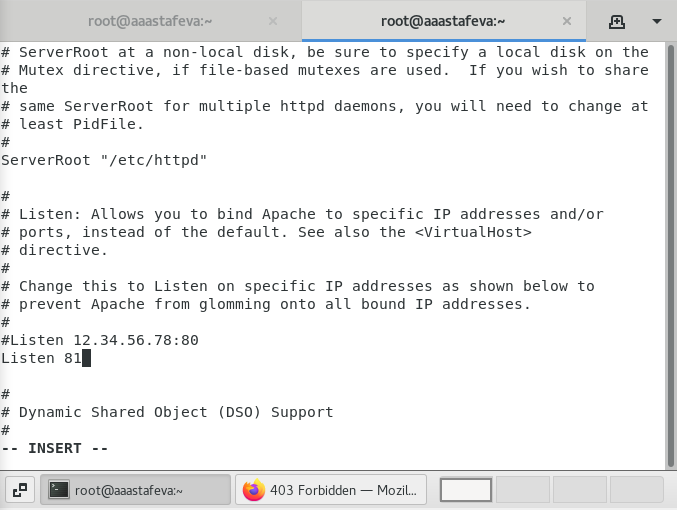


Figure 17: Изменеие порта 80 на 81

1. Проанализиировала лог-файлы. Просмотрела файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log. (рис. 18), (рис. 19), (рис. 20).

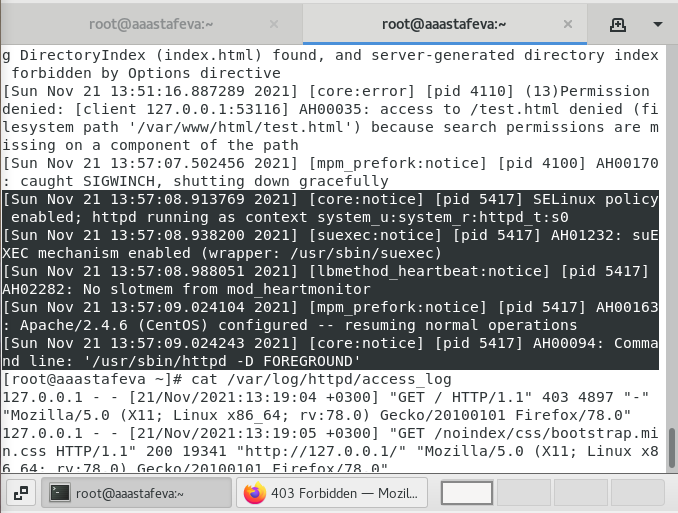


Figure 18: Анализ лог-файла

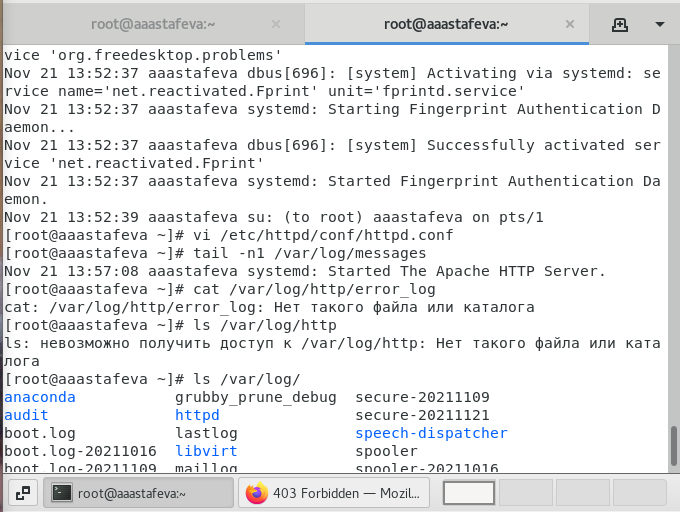


Figure 19: Анализ файла

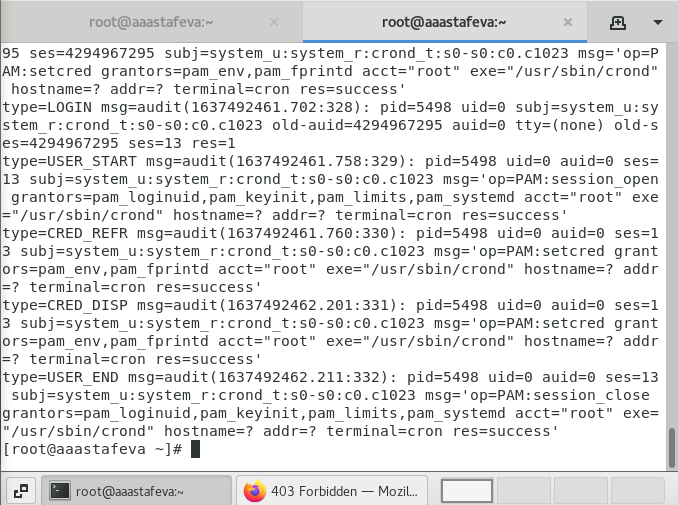


Figure 20: Анализ файла

1. Выполнила команду: semanage port -a -t http\_port\_t -р tcp 81. После этого проверила список портов командой: semanage port -l | grep http\_port\_t. Убедилась, что порт 81 появился в списке. (рис. 21).

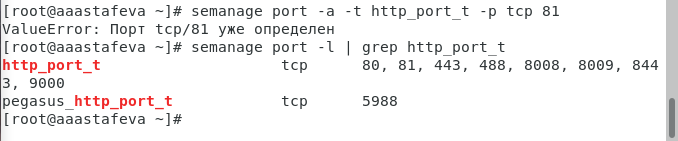


Figure 21: Выполнение и проверка

1. Вернула 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 попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Увидели содержимое файла — слово «test». (рис. 22), (рис. 23).

Figure 22: Возвращение контекста

Figure 22: Возвращение контекста

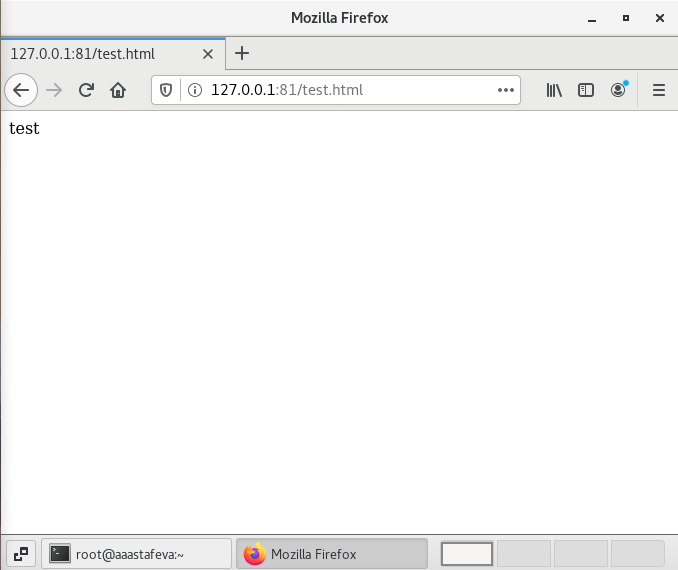


Figure 23: Получение доступа к файлу через браузер

1. Исправила обратно конфигурационный файл apache, вернув Listen 80. (рис. 24).

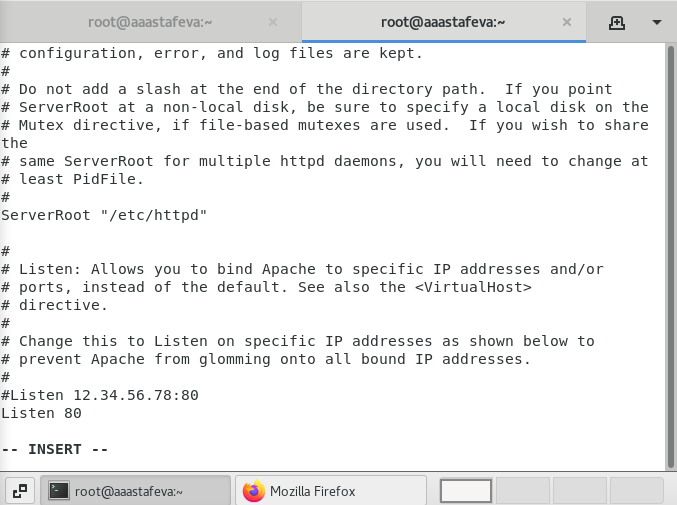


Figure 24: Исправление конфигурационного файл apache

1. Удалила привязку http\_port\_t к 81 порту. (рис. 25).

Figure 25: Удалние привязки http_port_t к 81 порту

Figure 25: Удалние привязки http\_port\_t к 81 порту

1. Удалила файл /var/www/html/test.html. (рис. 26).



Figure 26: Удаление файла /var/www/html/test.html

# Выводы

На основе проделанной работы развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinx на практике совместно с веб-сервером Apache.