Лабораторная работа №6

Мандатное разграничение прав в Linux

Дугаева Светлана Анатольевна

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.

# Подготовка лабораторного стенда

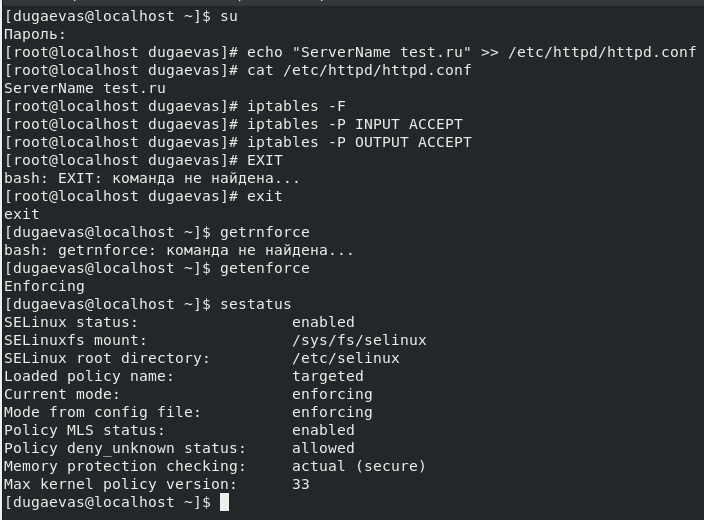
В конфигурационном файле /etc/httpd/httpd.conf необходимо задать параметр ServerName: ServerName test.ru чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе. Выполнила здание параметра с помощью команды echo “ServerName test.ru” >> /etc/httpd/httpd.conf

Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключила фильтр можно командами iptables -F iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT

# 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

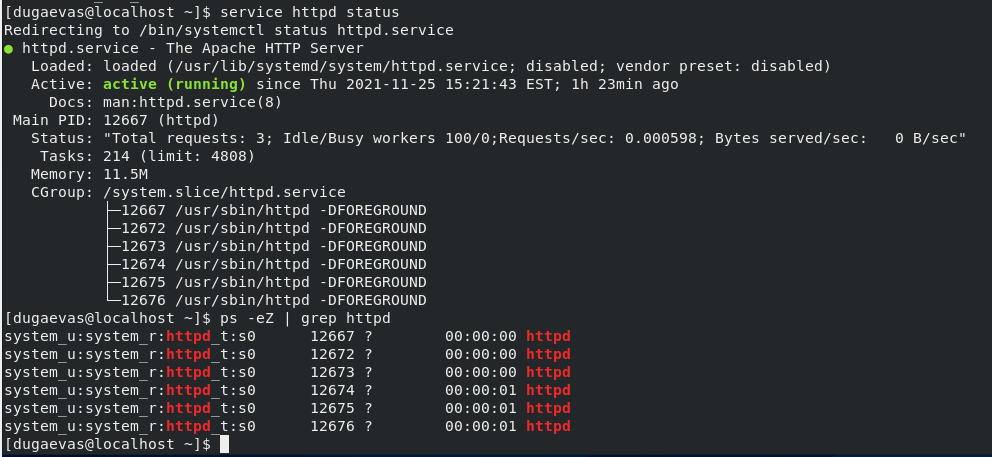
Действия из подготовки лабораторного стенда и пункта 1 выполнения лабораторной работы представленны на (рис. -@fig:001):



П. 1 выполения ЛР и подготовка

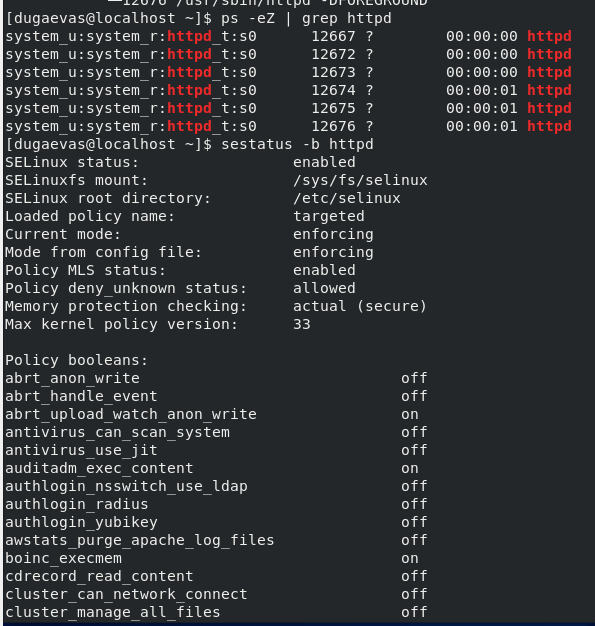
1. Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает: service httpd status
2. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности: пользователь system\_u, политика ролевого разделения system\_r, тип https\_t, уровень доступа s0.

Действия пунктов 2-3 предствленны на (рис. -@fig:002):



Статус веб-сервера и политика безопасности

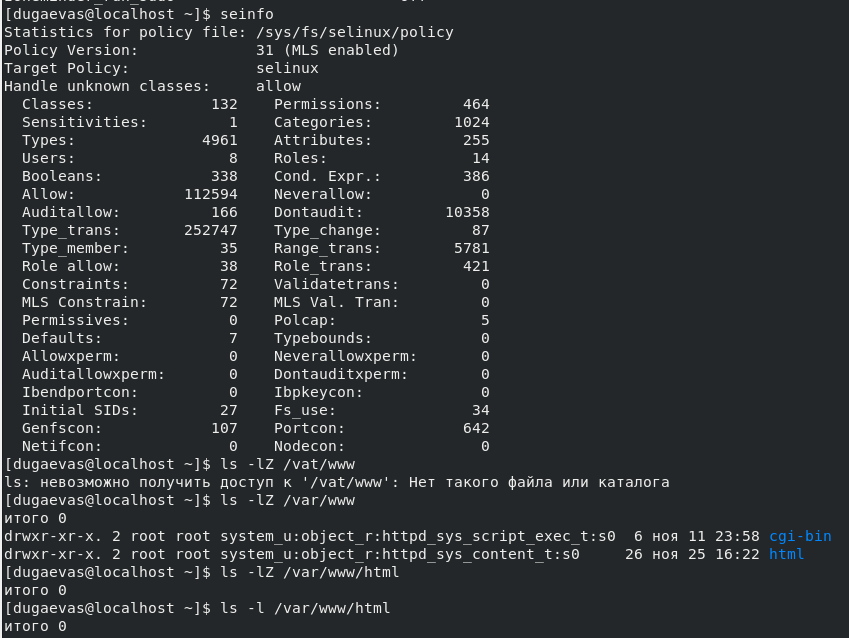
1. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды sestatus -b httpd Многие из них находятся в положении «off». (рис. -@fig:003):



Состояние переключателей

1. Посмотрела статистику по политике с помощью команды seinfo
2. Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www:
3. пределю тип файлов, находящихся в директории /var/www/html с помощью команды ls -lZ /var/www/html.
4. Определю круг пользователей, которым разрешено создание файлов в директории /var/www/html. Создавать файлы можно только суперпользователю, который является владельцем.

Действия пунктов 5-8 представленны на (рис. -@fig:004):



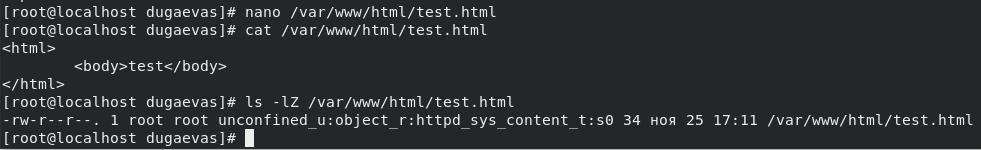
Пункты 5-8

1. Создам от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:

* test

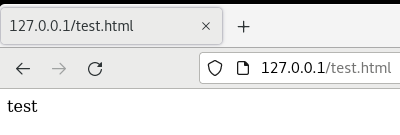
1. Проверю контекст созданного мной файла. По умолчанию вновь созданным файлам в директории /var/www/html присваивается контекст unconfined\_u:object\_r:httpd\_sys\_conent\_t:s0

Действия пунктов 9-10 представленны на (рис. -@fig:005):



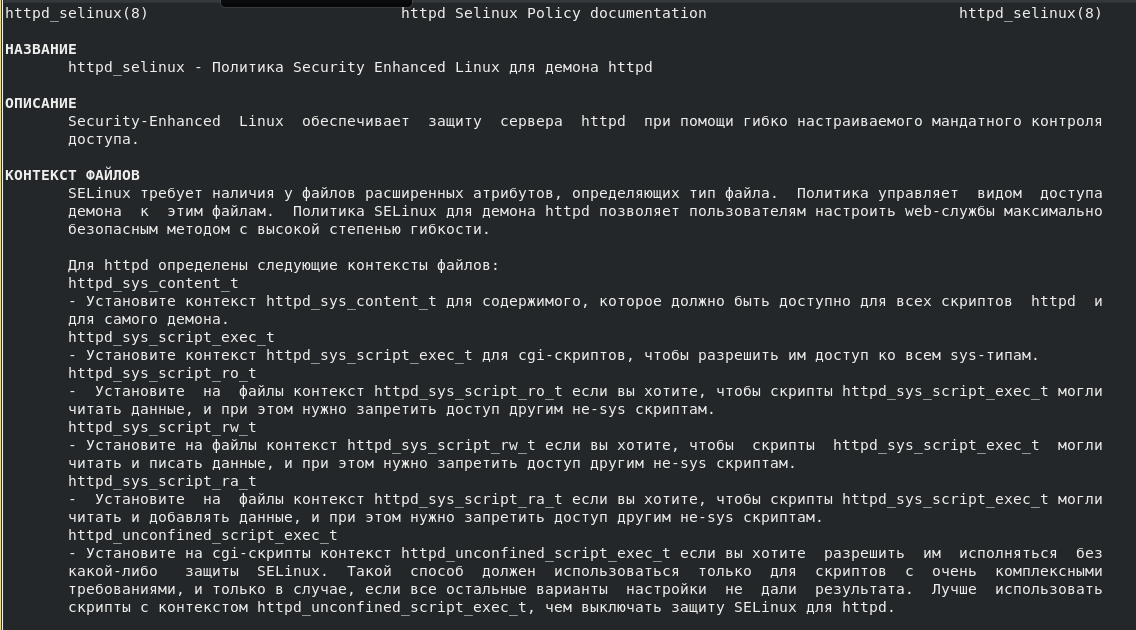
Пункты 9-10

1. Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Файл был успешно отображён (рис. -@fig:006):



Обращение к файлу через веб-сервер

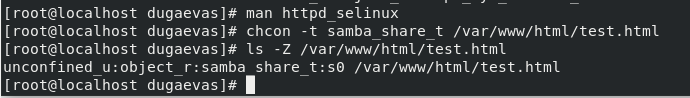
1. Изучила справку man httpd\_selinux (рис. -@fig:007):



Справка о контекстах

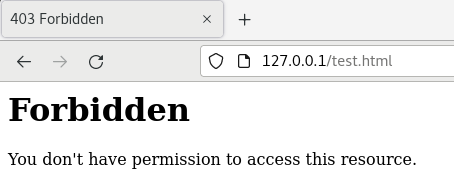
Контекст созданного мной файла: unconfined\_u : object\_r : httpd\_sys\_content\_t : s0, Тип httpd\_sys\_content\_t позволяет получить доступ к файлу, если мы обращаемся к нему через браузер.

1. Изменила контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t: (рис. -@fig:008):



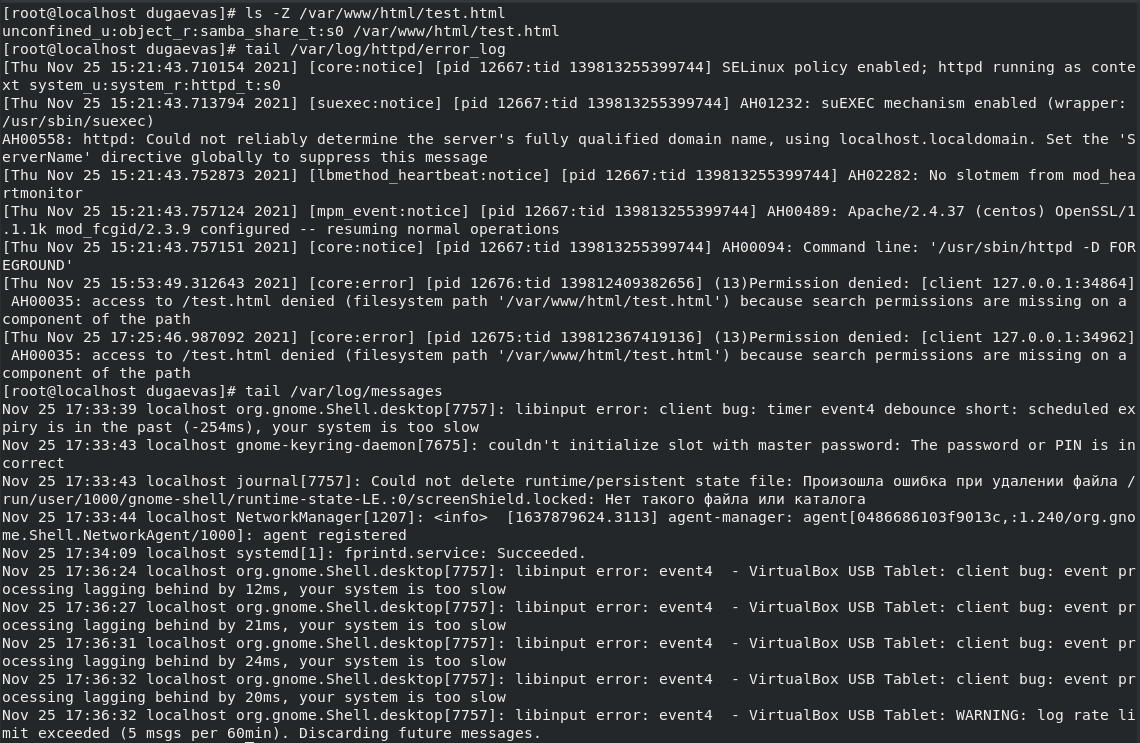
Изменение контекста

1. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html (рис. -@fig:009):



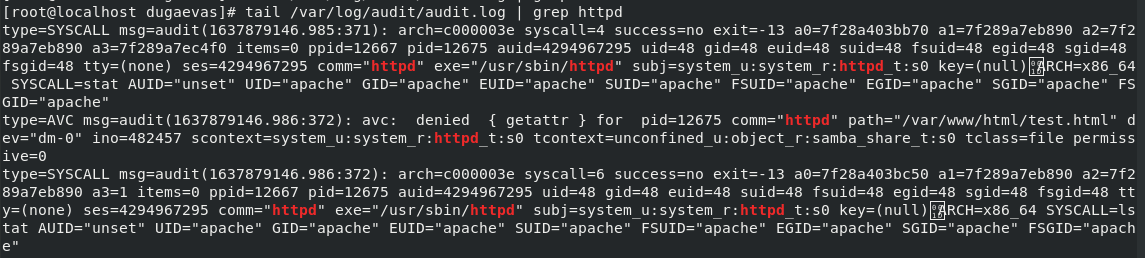
Доступ к файлу через веб-браузер

1. Файл не был отображен из-за того, что несмотря на возможность у любого пользователя просматривать файл, политика SELinux не задает правило, которое разрешало бы доступ, и операция сразу блокируется. Посмотрю log-файлы веб-сервера Apache и системный log файл (рис. -@fig:010):



log-файлы веб-сервера Apache и системный log файл

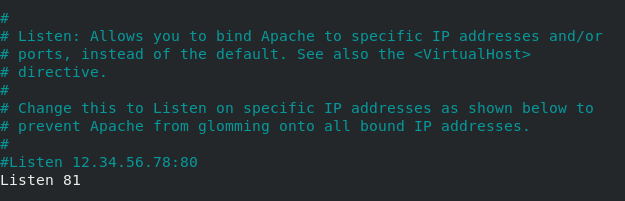
В системном log файле указано, что моя система слишком медленная, поэтому посмотрю ошибки в файле /var/log/audit/audit.log (рис. -@fig:011):



ошибки в файле audit.log

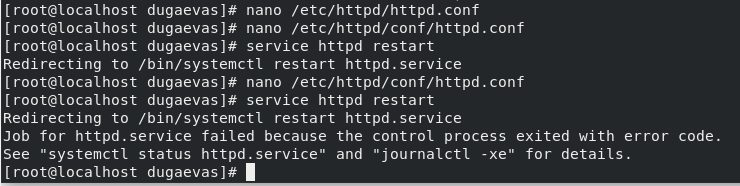
Сравнить ошибки не получилось из-за ошибки в чтении системного лог файла.

1. Попробовала запустить веб-сервер Apache на прослушивание ТСР-порта 81. Для этого в файле /etc/httpd/httpd.conf найду строчку Listen 80 и заменю 80 на 81 (рис. -@fig:012):



Смена порта

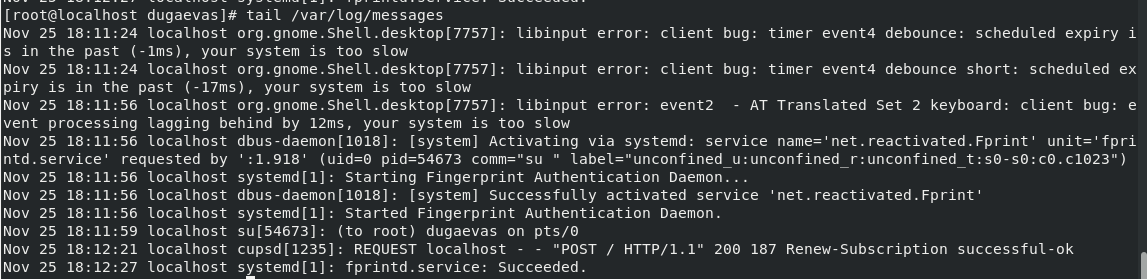
1. Выполнила перезапуск веб-сервера Apache. У меня сбоев не произошло. Возможно, это связано с тем, что данный порт зарезервирован и определен. Заменила 81 на 82. (рис. -@fig:013):



Перезапуск веб-сервера

Сбой произошел из-за того, что порт 82 не определен.

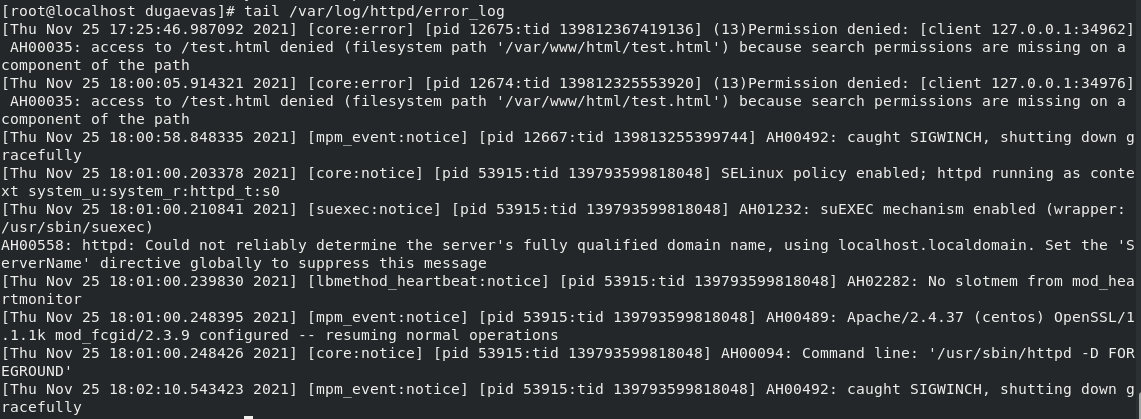
1. Проанализировала log файлы /var/log/messages (рис. -@fig:014):



log файлы /var/log/messages

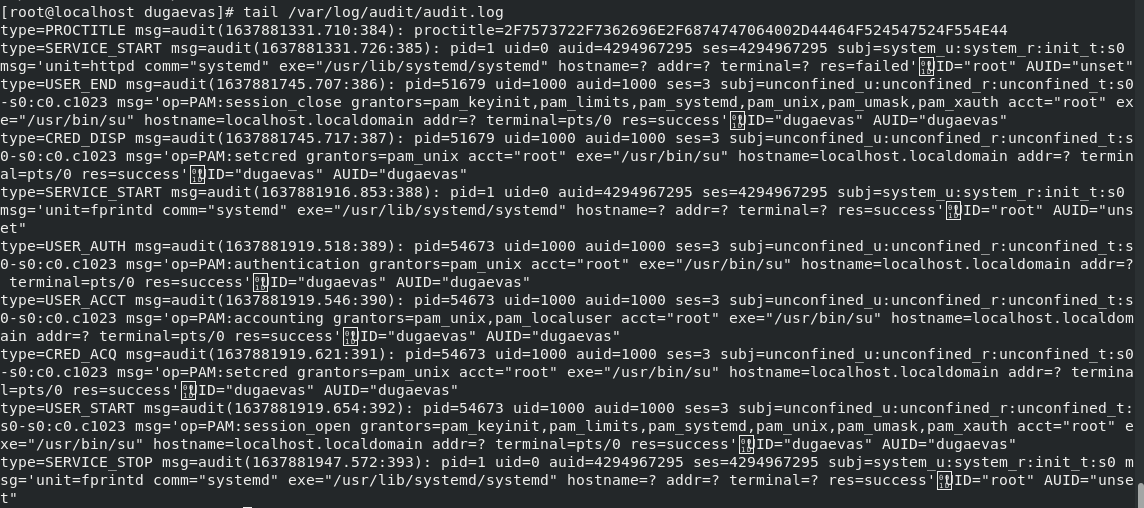
Снова ошибка, но я поискала информацию и определила, что подключение оборвалось, поскольку нет доступных сокетов и не получилось подключиться к адресу 0.0.0.82.

Просмотрела файл /var/log/http/error\_log: (рис. -@fig:015):



Файл error\_log

Просмотрю файл /var/log/audit/audit.log: (рис. -@fig:016):

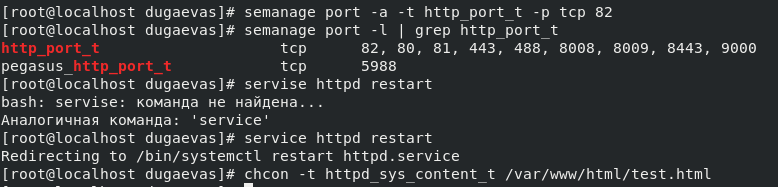


Файл audit.log

Новых сообщений не появилось.

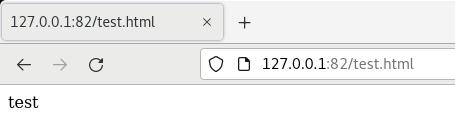
1. Выполнила команду semanage port -a -t http\_port\_t -р tcp 82: После этого проверила список портов командой semanage port -l | grep http\_port\_t:
2. Попробовала запустить веб-сервер Apache ещё раз. В этот раз запустить сервер получилось, поскольку на предыдущем шаге мы привязали новый порт.
3. Вернула контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html:

Действия пунктов 19-21 представленны на (рис. -@fig:017):



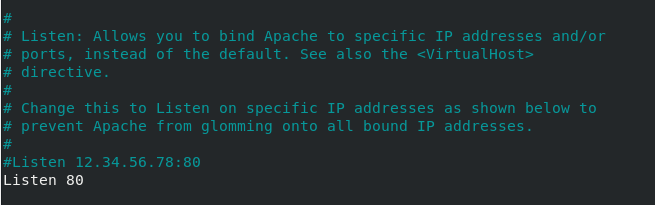
Пункты 19-21

Попробовала получить доступ к файлу /var/www/html/ test.html через браузер (рис. -@fig:018):



Доступ к файлу через веб-браузер

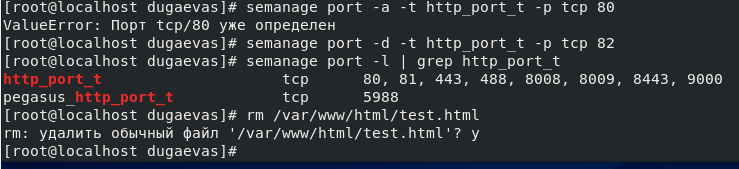
1. Исправила обратно конфигурационный файл apache, вернув Listen 80 (рис. -@fig:019):



Вернула конфиг. файл в первоначальное состояние

1. Удалила привязку http\_port\_t к 82 порту
2. Удалила файл /var/www/html/test.html

Действия пунктов 23-24 представленны на (рис. -@fig:020):



Пункты 23-24

# Выводы

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