Лабораторная работа №6: отчет.

Мандатное разграничение прав в Linux.

Евдокимов Максим Михайлович. Группа - НФИбд-01-20.

Содержание

# Цель работы

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

# Задание

1. Истоновить Apache и настроить его и систему для работы.
2. Изучить основы упровления и создания локалных сайтов.
3. Изучить основы SELinux и его работы совместно с веб-сервером Apache.

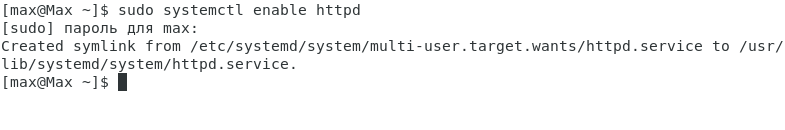
# Подготовка

## Пункт 1

Для проведения указанной лабораторной работы на одно рабочее место требуется компьютер с установленной операционной системой Linux, поддерживающей технологию SELinux. А также иметь устоновленный пакет Apache или его аналог httpd.

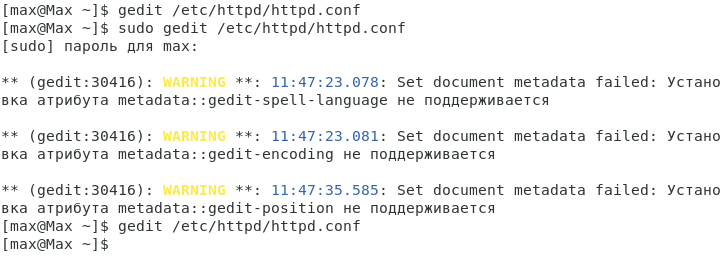
## Пункт 2

При необходимости администратор должен разбираться в работе SELinux и уметь как исправить конфигурационный файл /etc/selinux/config, так и проверить используемый режим и политику.



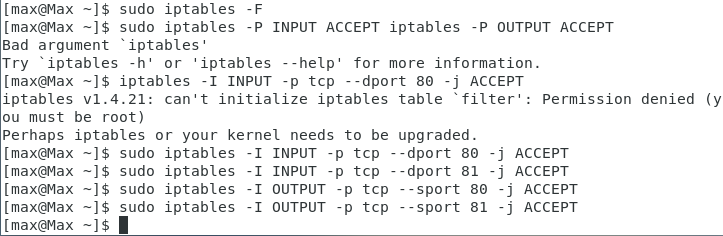
Подготовка к выполнению 1

В конфигурационном файле /etc/httpd/httpd.conf необходимо задать параметр ServerName “test.ru” чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе.



Подготовка к выполнению 2

Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp.

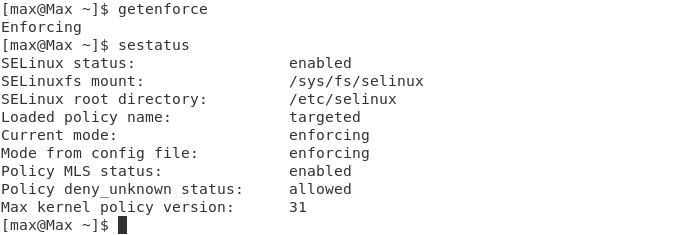


Подготовка к выполнению 3

# Выполнение лабораторной работы

## Пункт 1

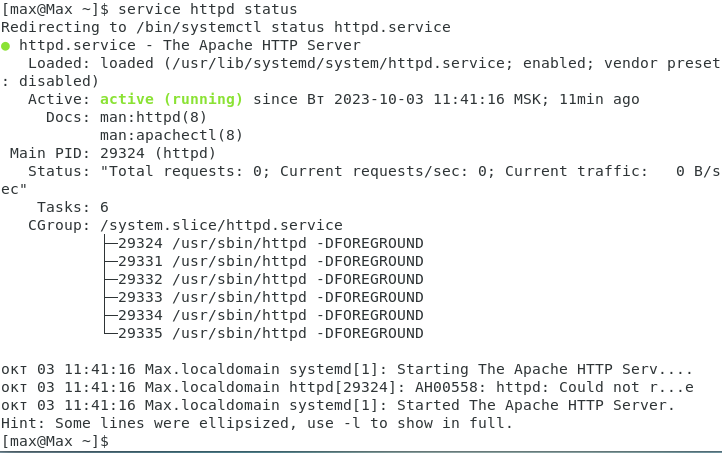
Воходим в систему с полученными учётными данными и убеждаемся, что SELinux работает в режиме enforcing политики targeted с помощью команд “getenforce” и “sestatus”.



Проверка параметров

## Пункт 2

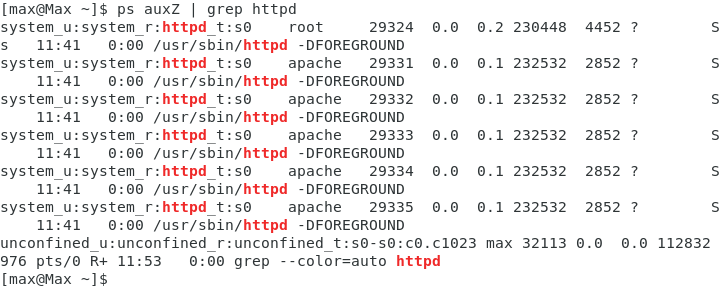
Обратимся с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает “service httpd status”.



ПРоверка веб-сервиса

## Пункт 3

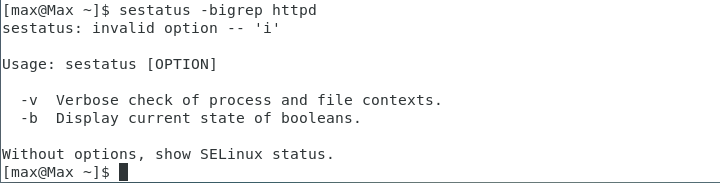
Найдём веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду “ps -eZ | grep httpd”



Находим сервис

## Пункт 4

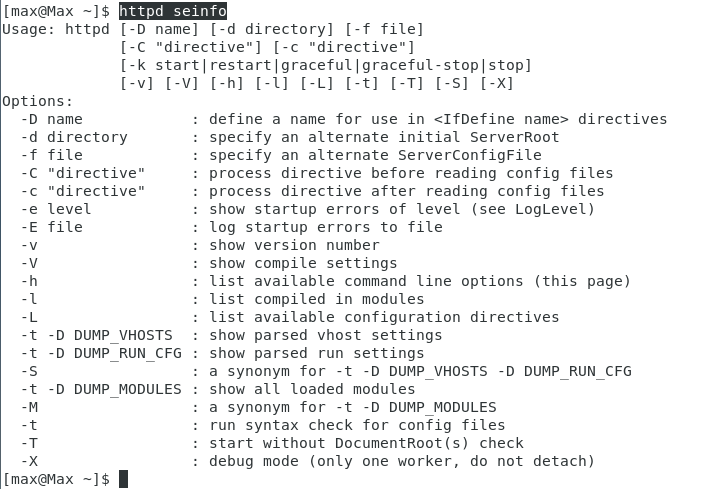
Посмотрим текущее состояние переключателей SELinux для Apache с помощью команды “sestatus -bigrep httpd”.



Проверка переключателей

## Пункт 5

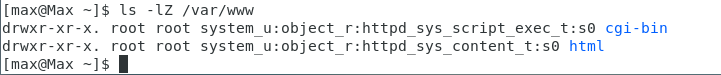
Посмотрим статистику по политике с помощью команды seinfo, такжеопределите множество пользователей, ролей, типов.



Просмотр статистики

## Пункт 6

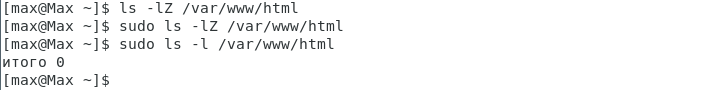
Определим тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды “ls -lZ /var/www”.



Анализ файлов в www

## Пункт 7

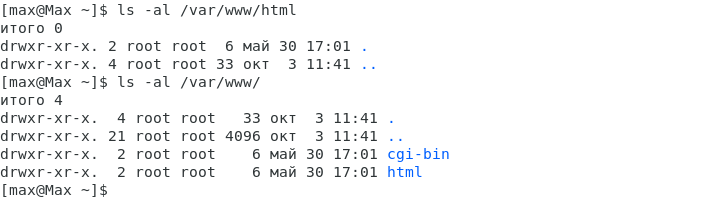
Определим тип файлов, находящихся в директории /var/www/html командой “ls -lZ /var/www/html”.



Анализ файлов в html

## Пункт 8

Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html командой “ls -al /var/www/html”.

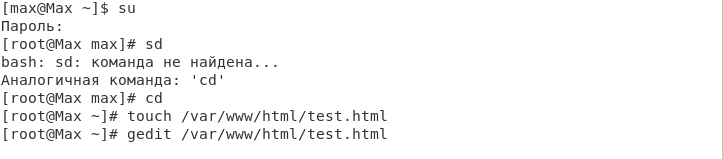


Проверка уровня допуска

## Пункт 9

Создаём от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

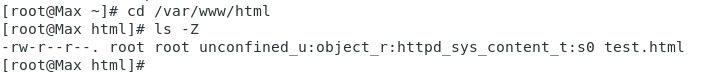
test



Создание локальной веб-страницы

## Пункт 10

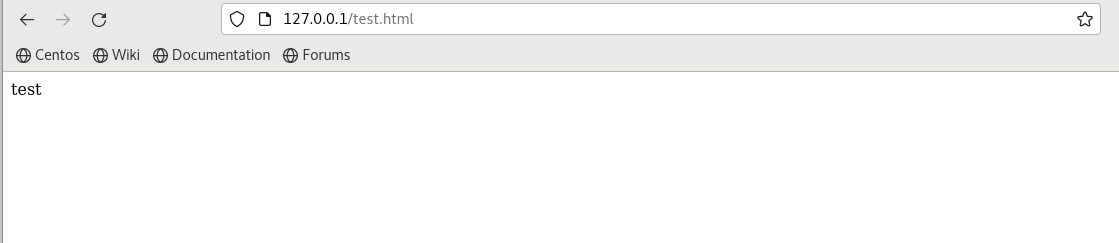
Проверим контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.



Проверка контекста

## Пункт 11

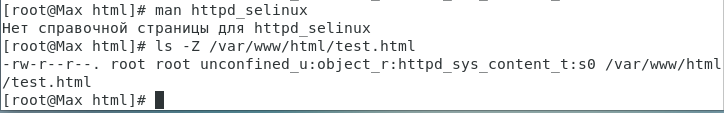
Обратимся к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”. Убедимся, что файл был успешно отображён.



Просмотр сайта

## Пункт 12

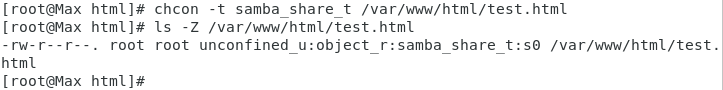
Изучем справку “man httpd\_selinux” и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html, проверив контекст файла можно командой “ls -Z /var/www/html/test.html”.



Изучаем справку

## Пункт 13

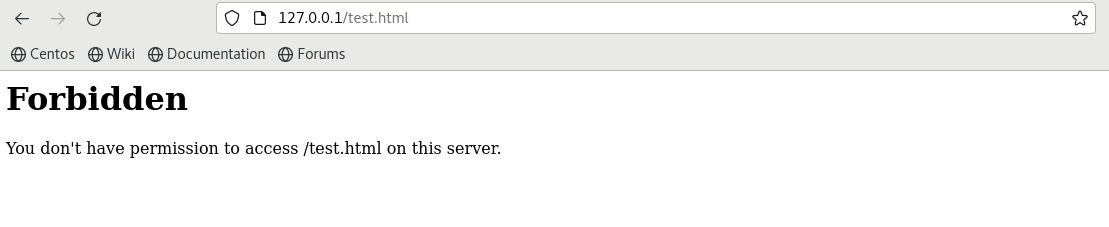
Измените контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba\_share\_t командами “chcon -t samba\_share\_t /var/www/html/test.html” и “ls -Z /var/www/html/test.html”.



Изменяем контекст

## Пункт 14

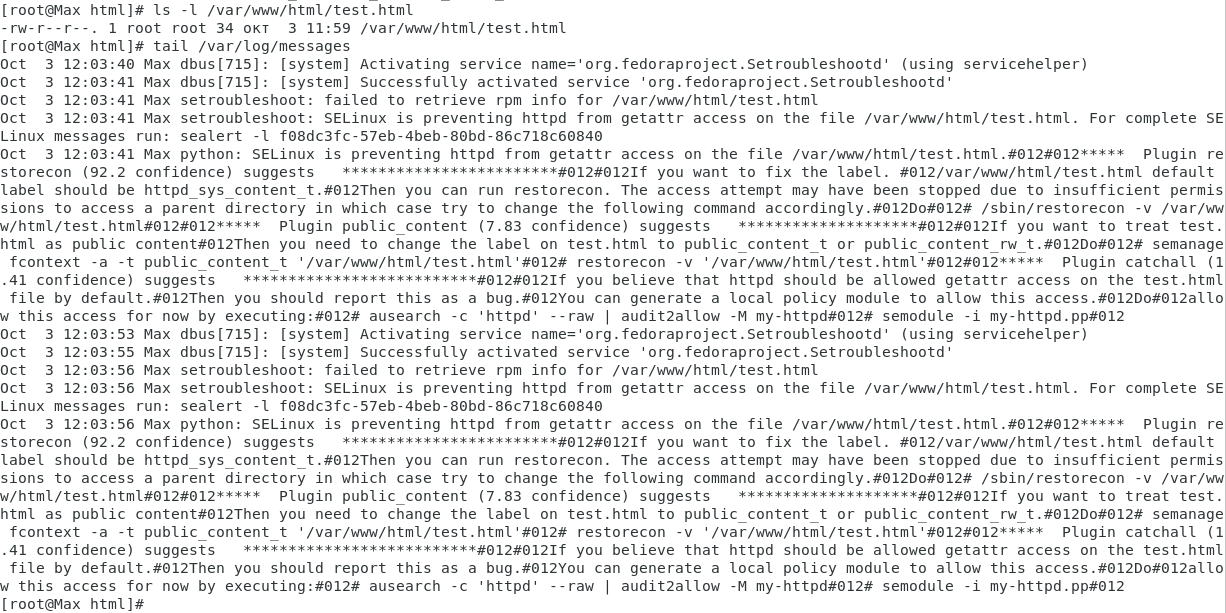
Попробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”. И получаем сообщение об ошибке Forbidden.



Пробуем зайти

## Пункт 15

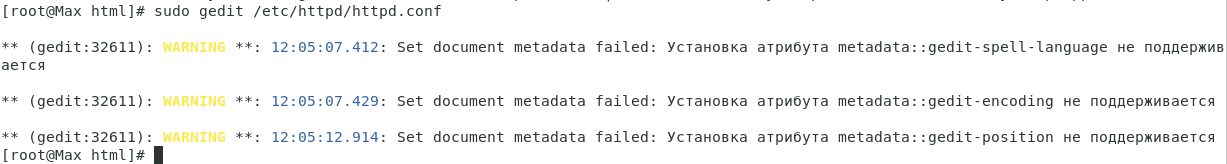
Проанализируем ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? “ls -l /var/www/html/test.html”. Просмотрим log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: “tail /var/log/messages”.



Проверяем доступ к файлу

## Пункт 16

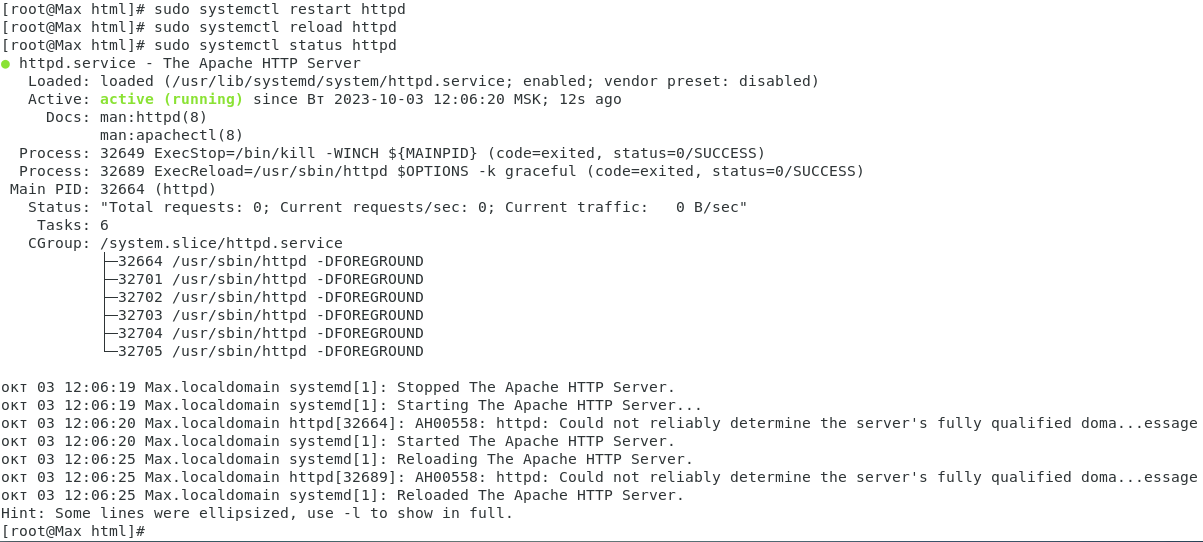
Запустим веб-сервер Apache на прослушивание ТСР-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81.



Запуск прослушивание

## Пункт 17

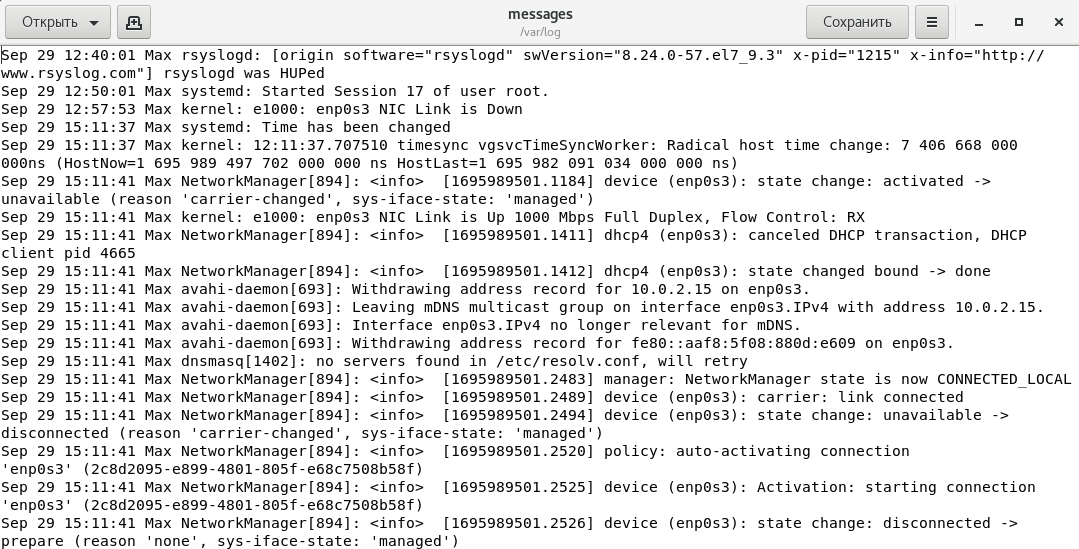
Выполнив перезапуск веб-сервера Apache.



Перезапуск веб-сервиса

## Пункт 18

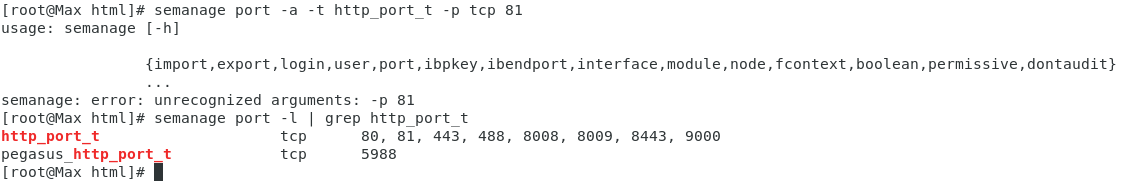
Проанализируем лог-файлы командой “tail -nl /var/log/messages”. Также просмотрим файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выясните, в каких файлах появились записи.



Анализ лог-файлов

## Пункт 19

Выполните команду “semanage port -a -t http\_port\_t -р tcp 81”. После этого проверьте список портов командой “semanage port -l | grep http\_port\_t”. Убедимся, что порт 81 появился в списке.



Активация порта

## Пункт 20

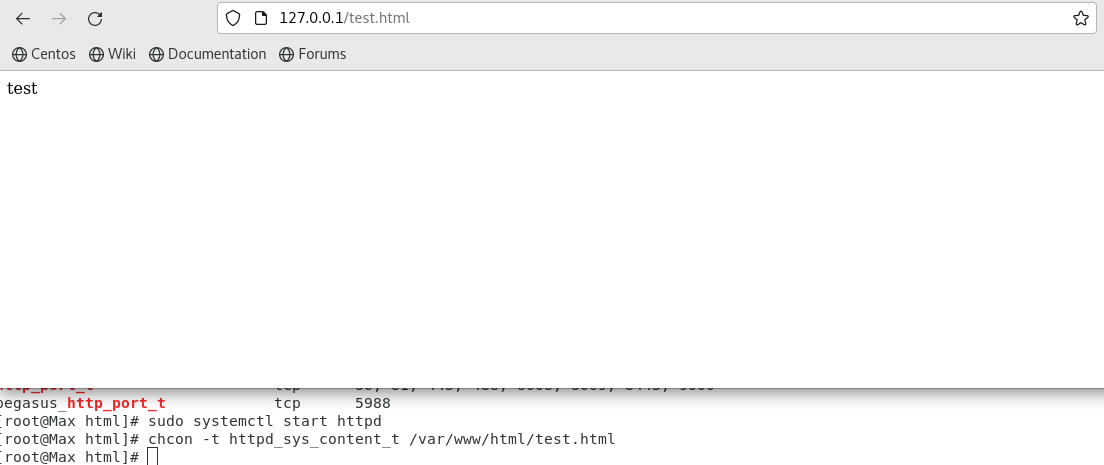
Пробуем запустить веб-сервер Apache ещё раз. И он работает.

Повторный запуск сайта

Повторный запуск сайта

## Пункт 21

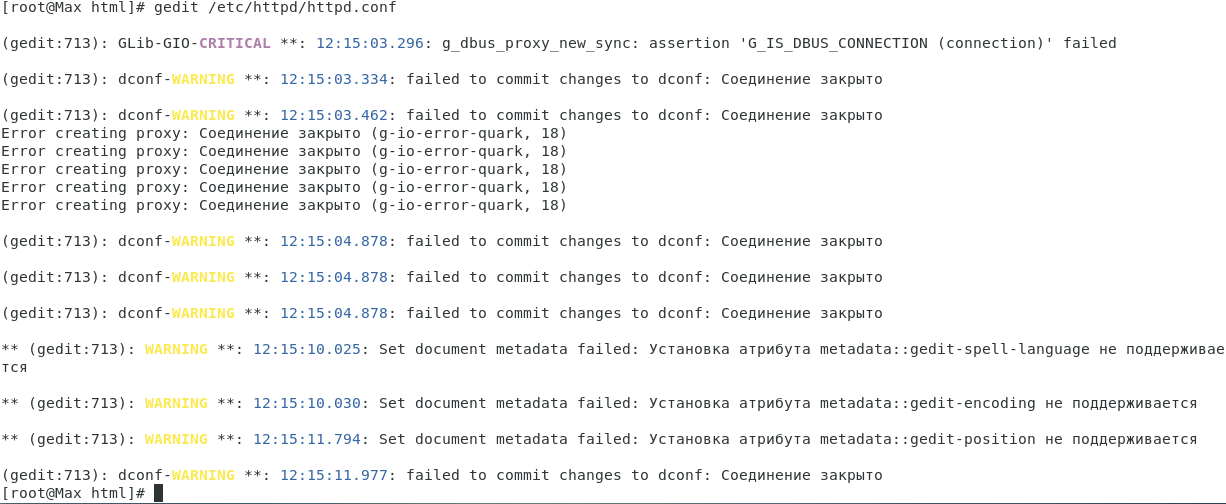
Вернём контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html: “chcon -t httpd\_sys\_content\_t /var/www/html/test.html”. После этого попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html.



Возвращаем изменения 1

## Пункт 22

Исправим обратно конфигурационный файл apache, вернув Listen 80.



Возвращаем изменения 2

## Пункт 23

Удалите привязку http\_port\_t к 81 порту: “semanage port -d -t http\_port\_t -p tcp 81” и проверьте, что порт 81 удалён.

Возвращаем изменения 3

Возвращаем изменения 3

## Пункт 24

Удалим файл /var/www/html/test.html командой “rm /var/www/html/test.html”.

Удаляем файл

Удаляем файл

# Выводы

В ходе работы был изучен пакет httpd (аналог apache), а также основы по работе с ним и с SELinux.

# Список литературы

1. [Лабораторная №6](https://esystem.rudn.ru/pluginfile.php/2090282/mod_resource/content/2/006-lab_selinux.pdf)
2. [Основы работы с SELinux](https://habr.com/ru/companies/otus/articles/460387/)
3. [Информация о работе с пакетными менеджерами](https://distroid.net/fix-apt-command-error-linux/)
4. [Устоновка Apache на CentOS через yum](https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-centos-7-ru)
5. [Работа с Apache/httpd](https://routerus.com/start-stop-restart-apache/)