Основы информационной безопасности

Лабораторная работа № 6. Мандатное разграничение прав в Linux

Нзита Диатезилуа Катенди

Содержание

# ПЦель работы

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

# Теоретические сведения

SELinux (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра[@habr\_selinux]. Впервые эта система появилась в четвертой версии CentOS, а в версиях 5 и 6 реализация была существенно дополнена и улучшена. Эти улучшения позволили SELinux стать универсальной системой, способной эффективно решать многие современные проблемы. Помните, что сначала применяется классическая система прав Unix, и управление перейдет к SELinux только в случае успешной первоначальной проверки.

Домен — это список действий, которые может выполнять процесс. Обычно домен определяется как минимально возможный набор действий, с помощью которых может функционировать процесс. Таким образом, если процесс дискредитирован, злоумышленник не сможет нанести большого ущерба.

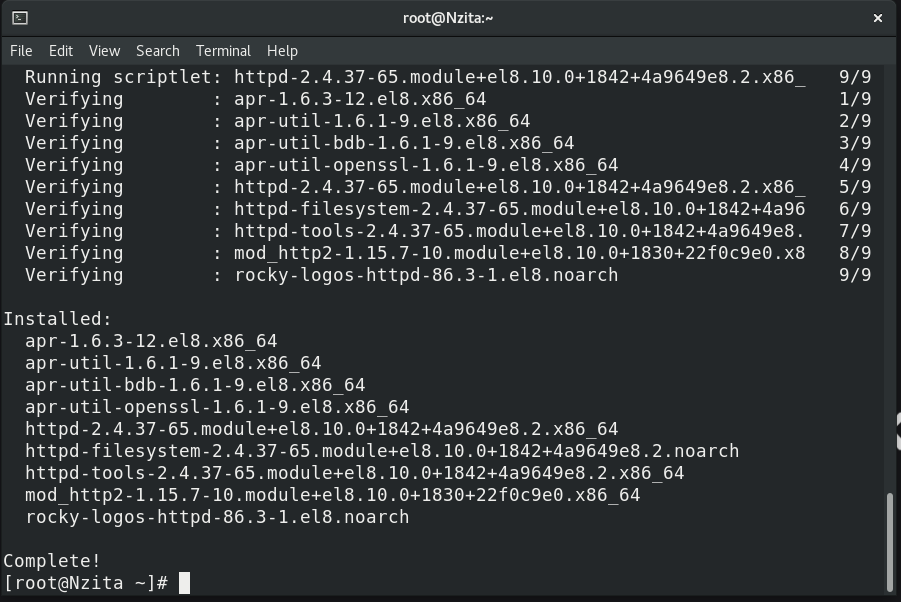
Функция — это список доменов, которые можно применить. Если заданный домен отсутствует в списке доменов роли, действия из этого домена не могут быть применены.

Тип — это набор разрешенных действий по отношению к объекту. Тип отличается от домена тем, что его можно применять к каналам, каталогам и файлам, тогда как домен применяется к процессам.

Контекст безопасности – все атрибуты SELinux – роли, типы и домены.

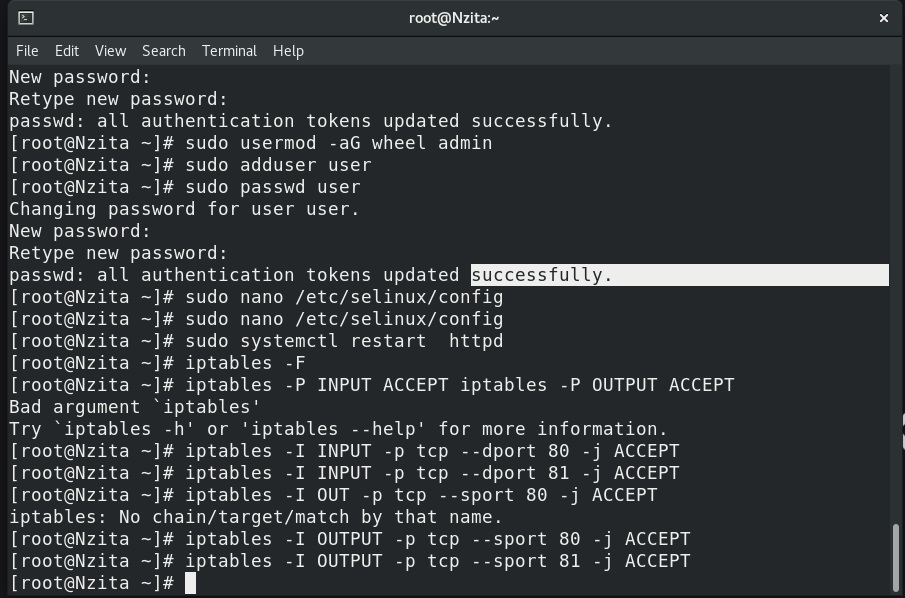
# Выполнение лабораторной работы

В конфигурационном файле /etc/httpd/httpd.conf зададим параметр ServerName. Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключим фильтр командами(рис. @fig:001)



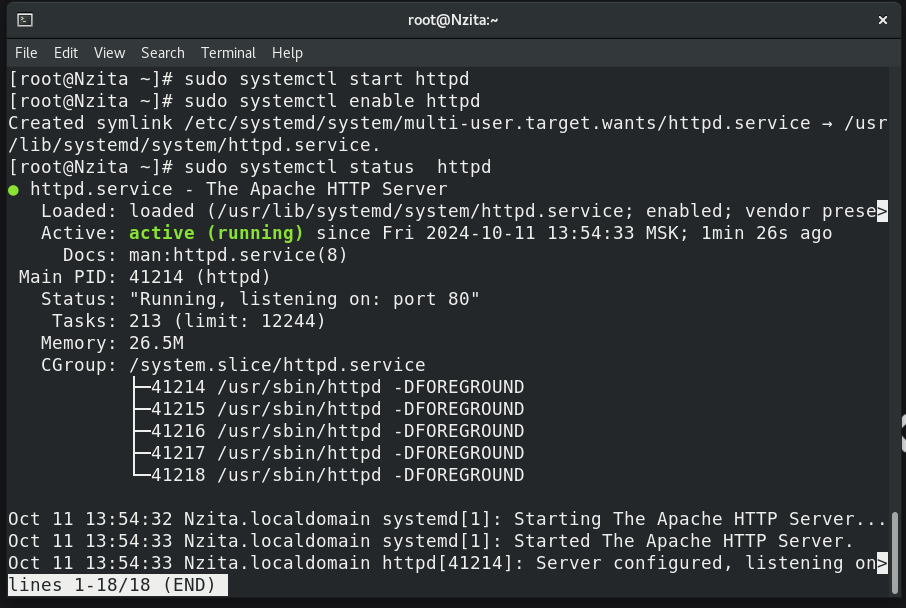
Подготовка лабораторного стенда

Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus(рис. @fig:002).



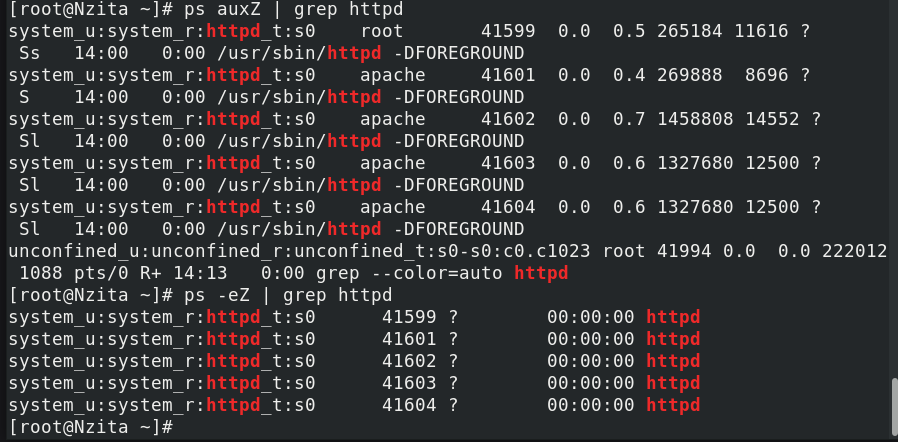
Проверка статуса SELinux

Обратимся с помощью браузера к веб-серверу, запущенному на нашем компьютере, и убедитесь, что последний работает(рис. @fig:003).



Проверка статуса веб-сервера

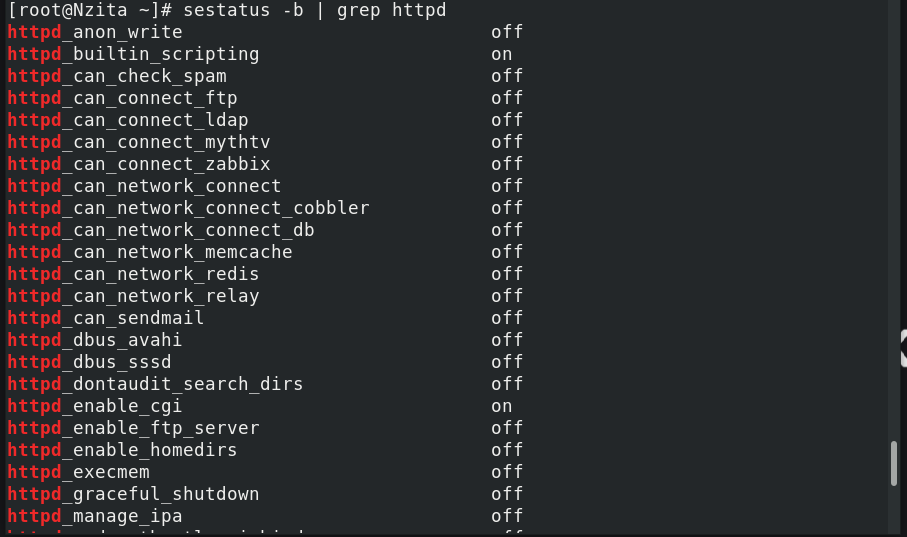
Найдите веб-сервер Apache в списке процессов, определим его контекст безопасности(рис. @fig:004)



Просмотр контекста безопасности веб-сервера

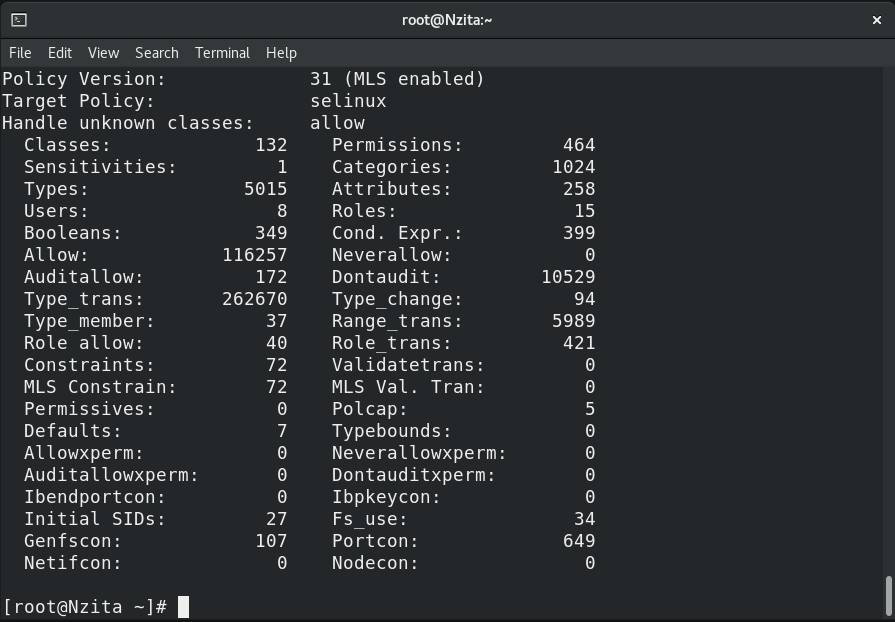
Мы можем видеть контекст безопасности SELinux: system\_u:system\_r:httpd\_t.

Посмотрим текущее состояние переключателей SELinux для Apache(рис. @fig:005)



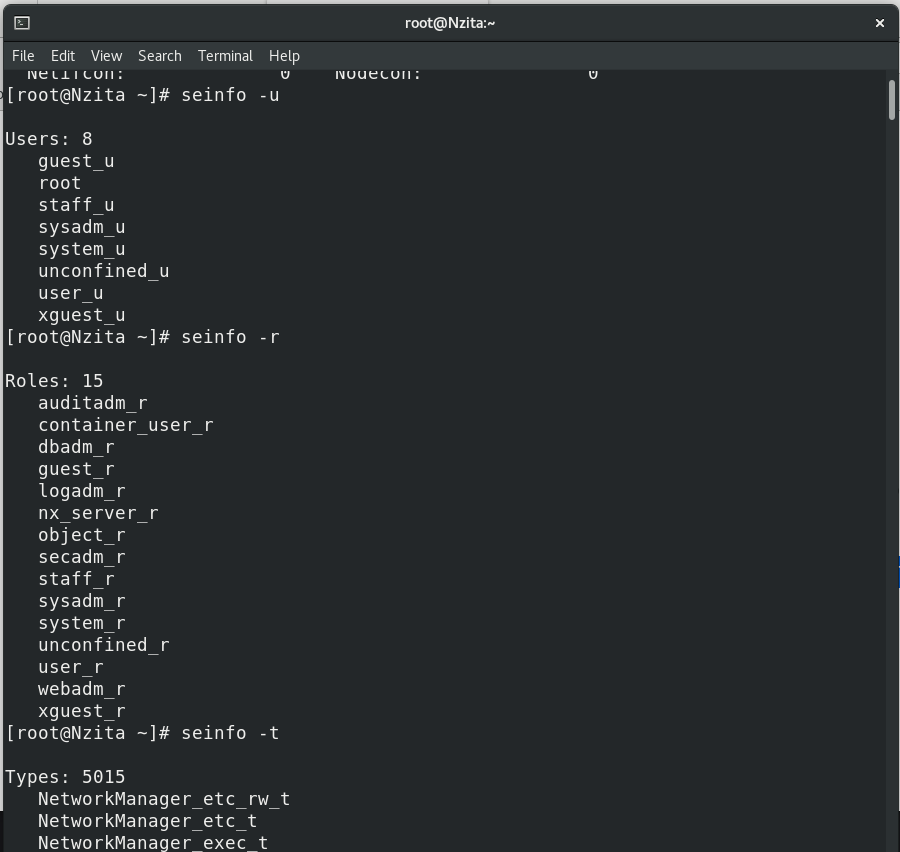
Состояние переключателей SELinux для Apache

Посмотрим статистику по политике с помощью команды seinfo(рис. @fig:006):



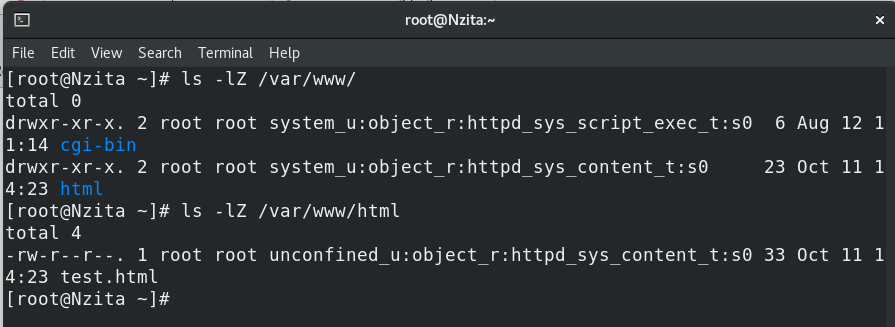
Статистика по политике

Также просмотрим множество пользователей, ролей, типов(рис. @fig:007):



Множества пользователей, ролей, типов

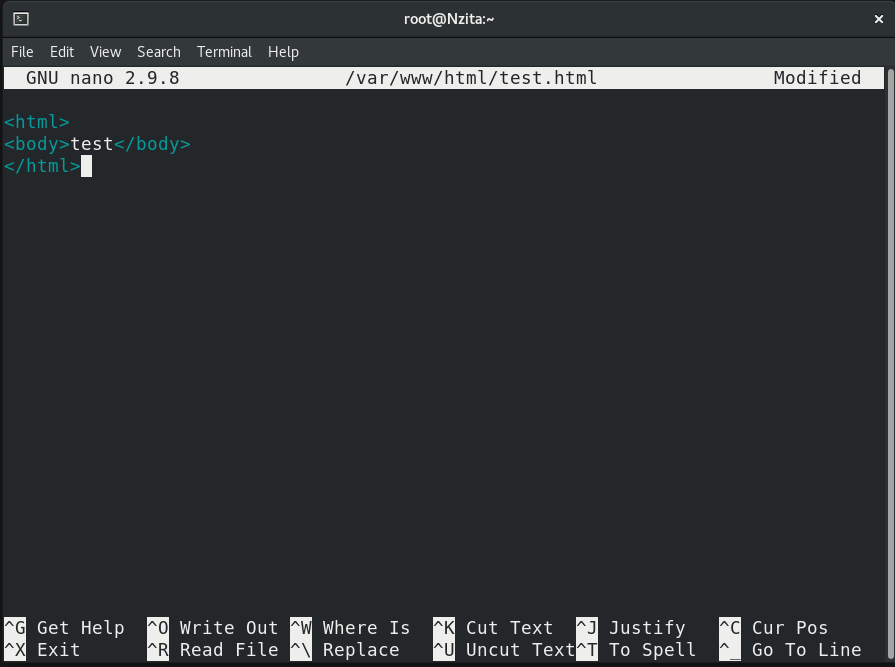
Определив тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www, увидим, что есть директория, содержащая cgi-скрипты, и директория /var/www/html, содержащая все скрипты httpd(в данный момент пустая)(рис. @fig:008):



Просмотр типов директорий в /var/www

Можно увидеть, что создание файлов в директории /var/www/html разрешено только владельцу – root.

Создадим 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. @fig:009):



Содержимое html-файла /var/www/html/test.html

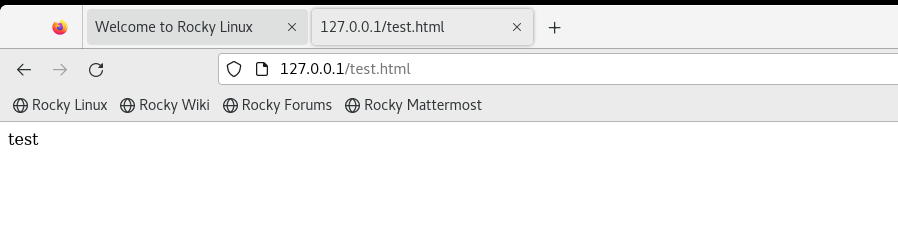
Затем посмотрим контекст безопасности, который был задан по умолчанию этому файлу(@fig:010):



Установка пароля для пользователя с правами администратора

Увидим, что файлам по умолчанию сопоставляется свободный пользователь SELinux unconfined\_u, указана роль object\_r используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах и тип httpd\_sys\_content\_t, который позволяет процессу httpd получить доступ к файлу

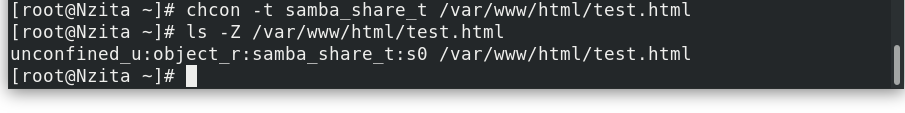
Обратимся к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html, убедимся, что файл был успешно отображён.(рис. @fig:011):



Открытие html-страницы через браузер

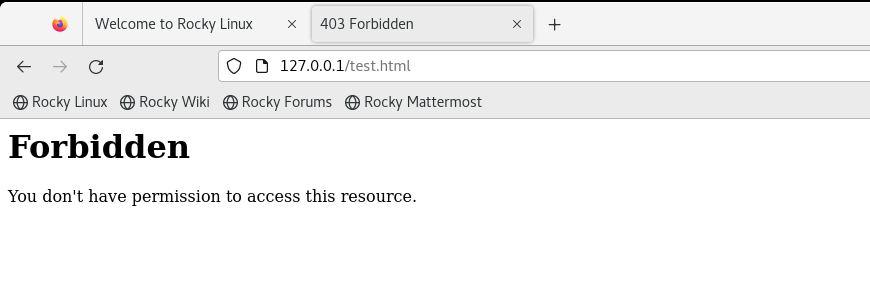
Изучив справку man httpd\_selinux, выясним, какие контексты файлов определены для httpd. Сопоставив их с типом файла test.html увидим, что его контекст httpd\_sys\_content\_t для содержимого, которое должно быть доступно для всех скриптов httpd и для самого демона.

Изменим контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на тот, к которому процесс httpd не должен иметь доступа – samba\_share\_t(рис. @fig:012):



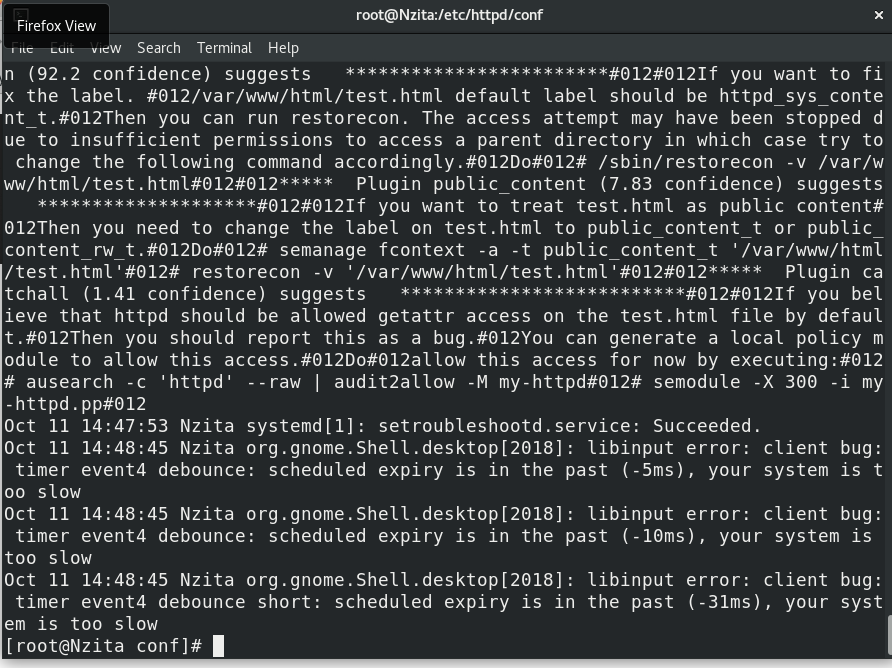
Изменение контекста файла /var/www/html/test.html

Теперь снова попробуем получить доступ к файлу через браузер и получим отказ(рис. @fig:013):



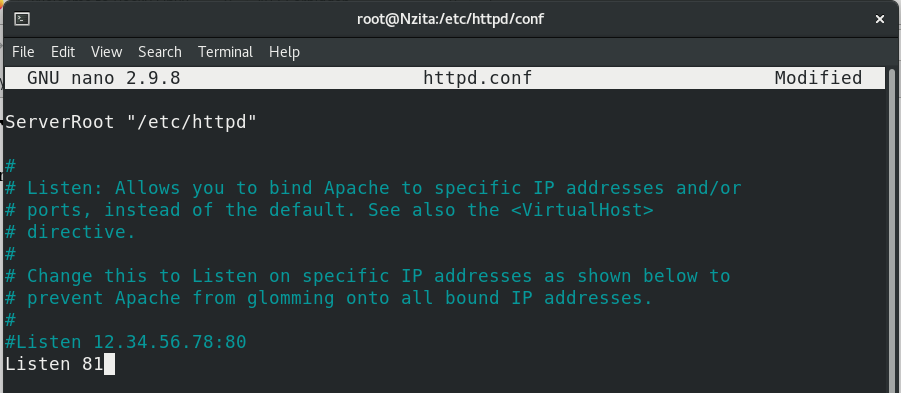
Отказ в доступе к html-странице через браузер

Посмотрим log-файлы веб-сервера Apache и системный лог-файл и увидим, что отказ происходит, так как доступ запрещен SELinux именно к веб-серверу(на просто просмтр текстовых файлов это не влияет)(рис. @fig:014):



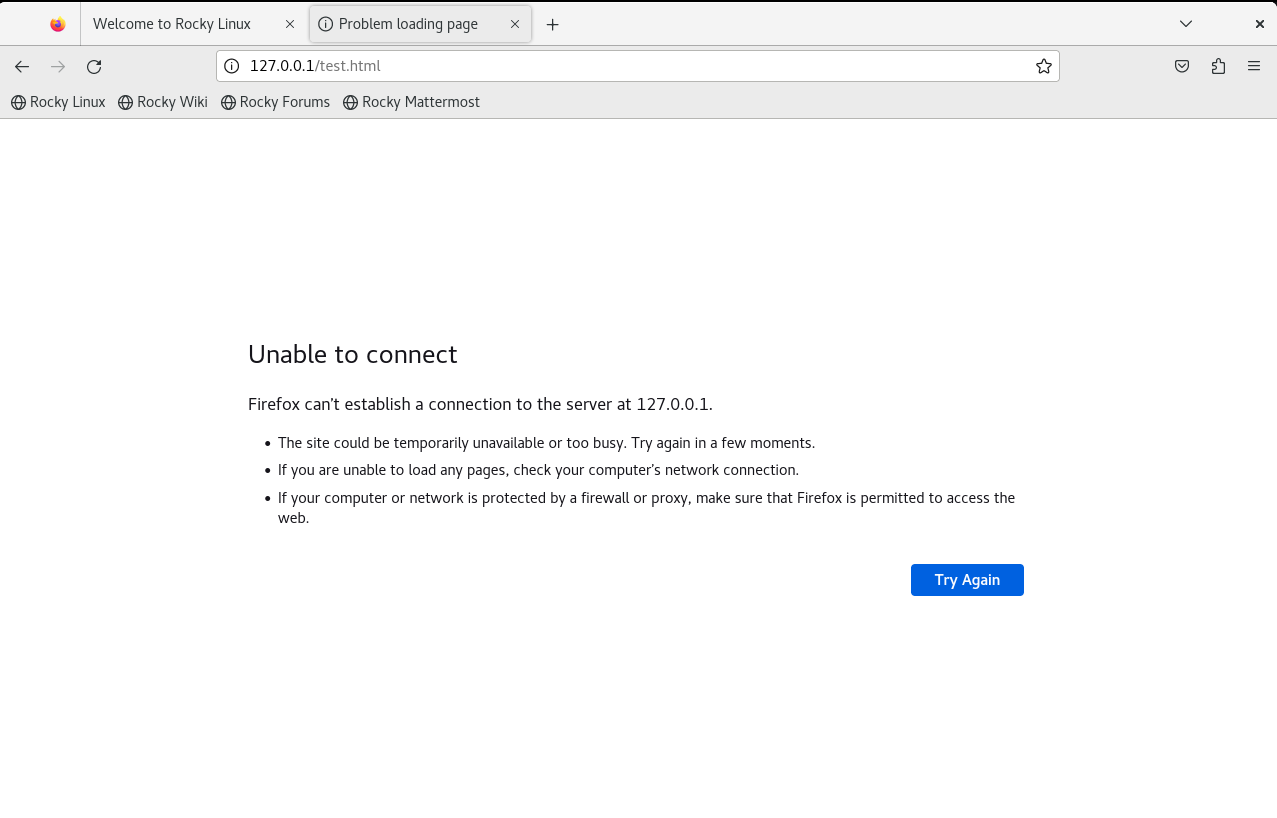
Просмотр лог-файлов

Запустим веб-сервер Apache на прослушивание ТСР-порта 81. Для этого в файле /etc/httpd/httpd.conf найдем строчку Listen 80 и заменим её на Listen 81(рис. @fig:015):



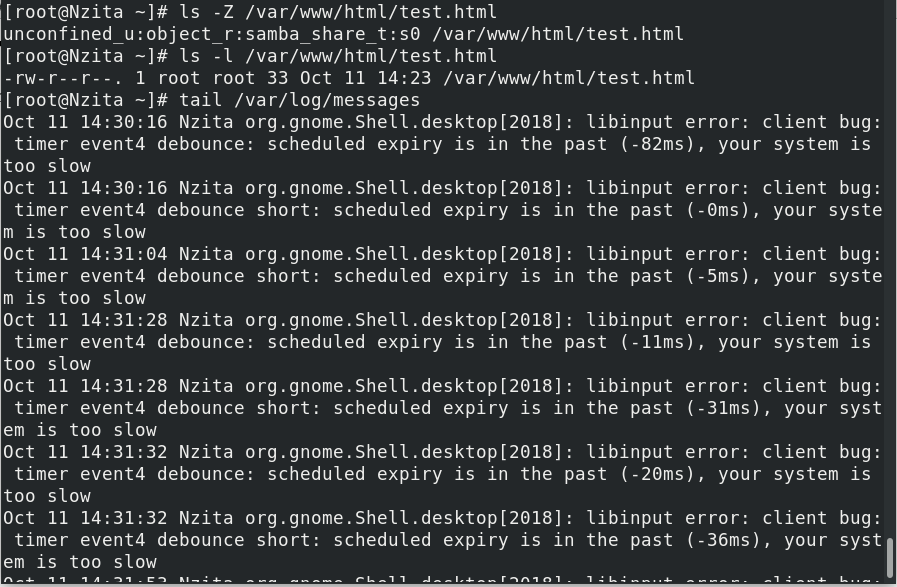
Замена прослушиваемого порта

Выполниv перезапуск веб-сервера Apache и увидим предупреждение безопасности, так как 81 порт не является официальным портом для доступа по TCP(рис. @fig:016):



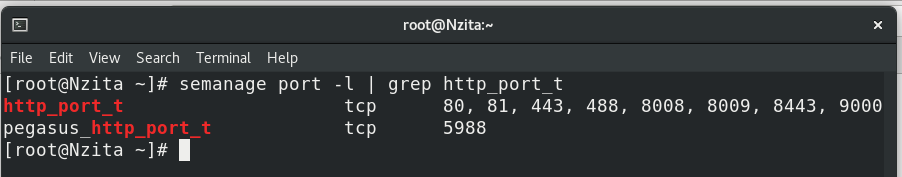
Открытие html-страницы через браузер при прослушивании 81 порта

Просмотрев лог-файлы увидим, что порт для прослушивания был сменен(рис. @fig:017):



Просмотр лог-файлов

Также этот порт мог быть отклчен, тогда мы бы совсем не видели страницу, добавлять порты и просматривать актуальные можно с помощью команды seamanage(рис. @fig:018):



Просмотр портов с помощью seamnage

В конце работы вернем все сделанные изменения в файлах конфигурации веб-сервера.

# Выводы

В результате выполнения работы были приобретены практические навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux. Проверена работа SELinx на практике совместно с веб-сервером Apache.

# Список литературы