Лабораторная работа №6

Мандатное разграничение прав в Linux

Роман Владимирович Иванов

Содержание

# Цель работы

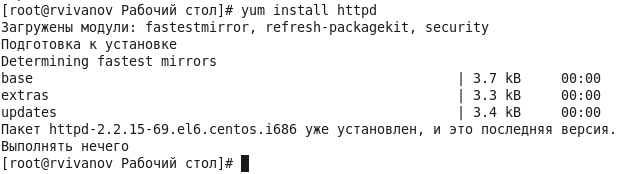
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. [1]  
Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Задание

1. Подготовить лабораторный стенд и ознакомиться с методическими рекомендациями.
2. С помощью различных примеров ознакомиться с работой SELinux и веб-сервисом Apache.

# Выполнение лабораторной работы

1. Подготовил лабораторный стенд и ознакомился с методическими рекомендациями.  
   Предварительно установил веб-сервис Apache с помощью команды (рис - @fig:001).

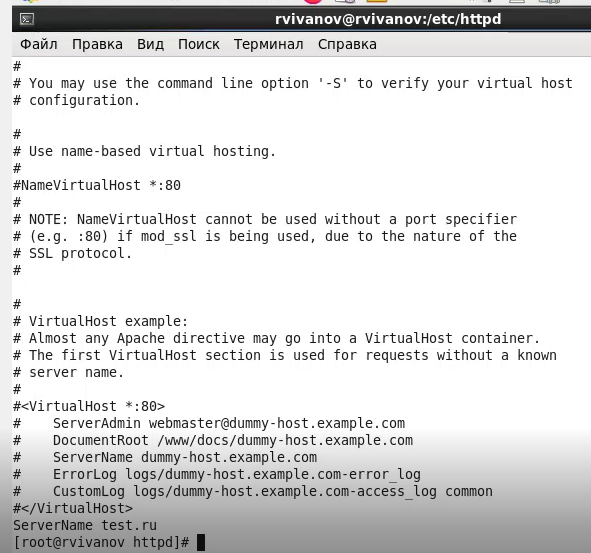


Установка Apache

В конфигурационном файле задал параметр ServerName: . Это делается для того, чтобы при запуске веб-сервиса не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе (рис - @fig:002 и @fig:003).

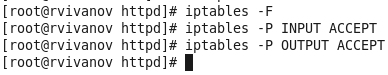
Внемение информации в конфигурационный файл

Внемение информации в конфигурационный файл



Чтение конфигурационного файла

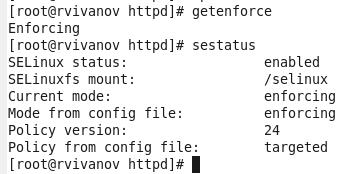
Также отключил пакетный фильтр (рис - @fig:004).



Отключение пакетного фильтра

1. С помощью различных примеров ознакомился с работой SELinux и веб-сервисом Apache.

Вошел в систему с полученными учетными данными и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд и (рис - @fig:005).



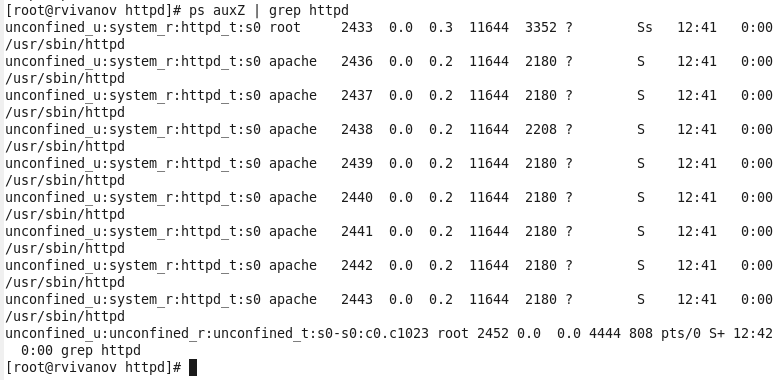
Проверка режима работы SELinux

Обралится с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедился, что последний работает с помощью команды , предварительно запустив его с помощью команды (рис - @fig:006).



Проверка работы веб-сервера

Нашел веб-сервер Apache в списке процессов и определил его контекст безопасности с помощью команды (рис - @fig:007).



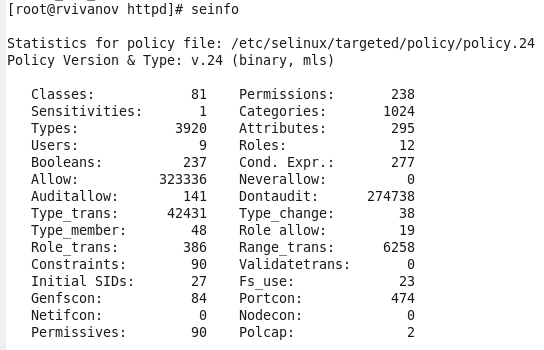
Поиск веб-сервера Apache и определение его контекста безопасности

Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды (рис - @fig:008). Многие из низ находятся в положении “off”.



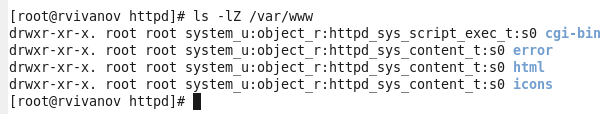
Ттекущее состояние переключателей SELinux для Apache

Посмотрел статистику по политике с помощью команды , а также определил множество пользователей, ролей, типов (рис - @fig:009).



Статистика по политике

Определил тип файлов и поддиректорий, находящихся в директории , с помощью команды (рис - @fig:010).



Определение типов файлов и поддиректорий, находящихся в директории

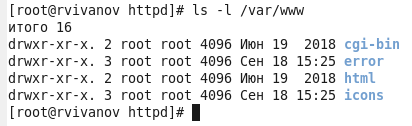
Определил тип файлов, находящихся в директории с помощью команды (рис - @fig:011).

Определение типов файлов и поддиректорий, находящихся в директории 

Определение типов файлов и поддиректорий, находящихся в директории

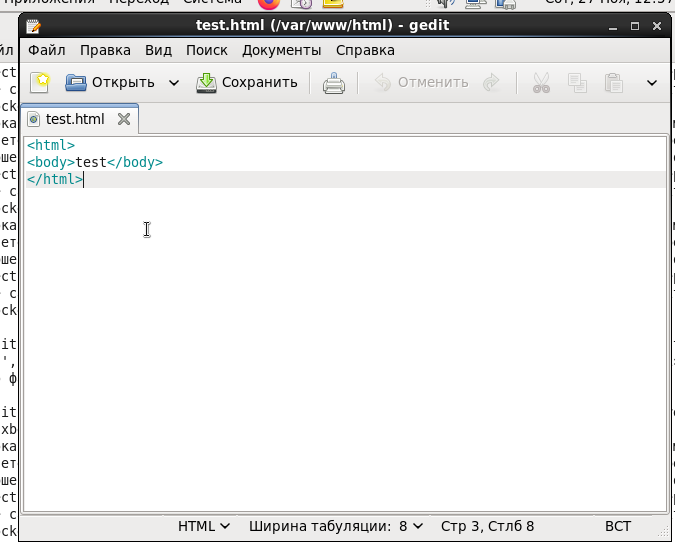
Консоль ничего не выводит, поскольку дирректория пуста.

Определил круг пользователей, которым разрешено создание файлов в директории (рис - @fig:012).



Пользователи, которым разрешено создание файлов в директории

Создал от имени суперпользователя html-файл следующего содержания (рис - @fig:013):



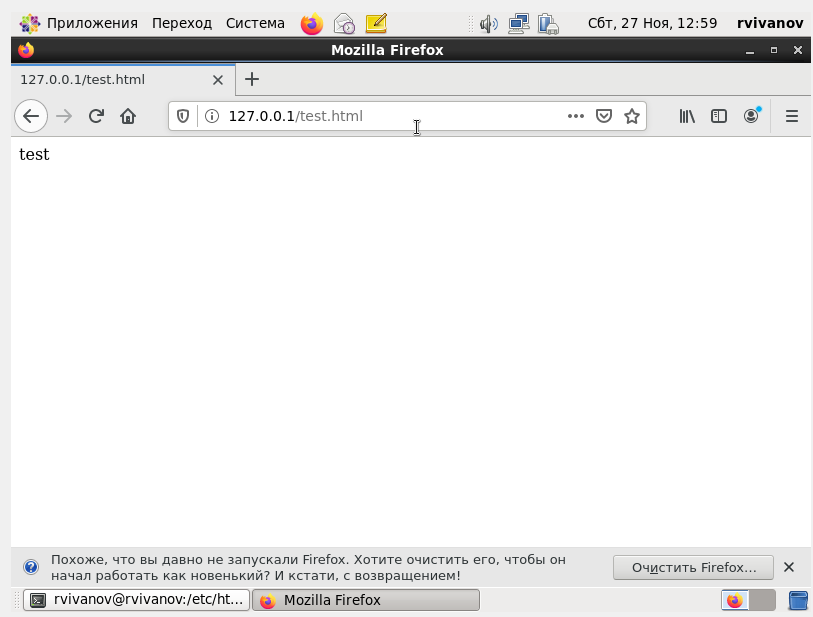
html-файл и его содержимое

Проверил контекст созданного мною файла (рис - @fig:014):

Контекст html-файл

Контекст html-файл

Обратился к файлу через веб-сервис, введя в браузере адрес (рис - @fig:015):



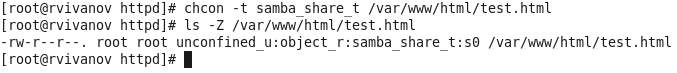
Обращение к файлу через браузер

Проверил контекст файла с помощью команды (рис - @fig:016).

Выяснение контекста файла

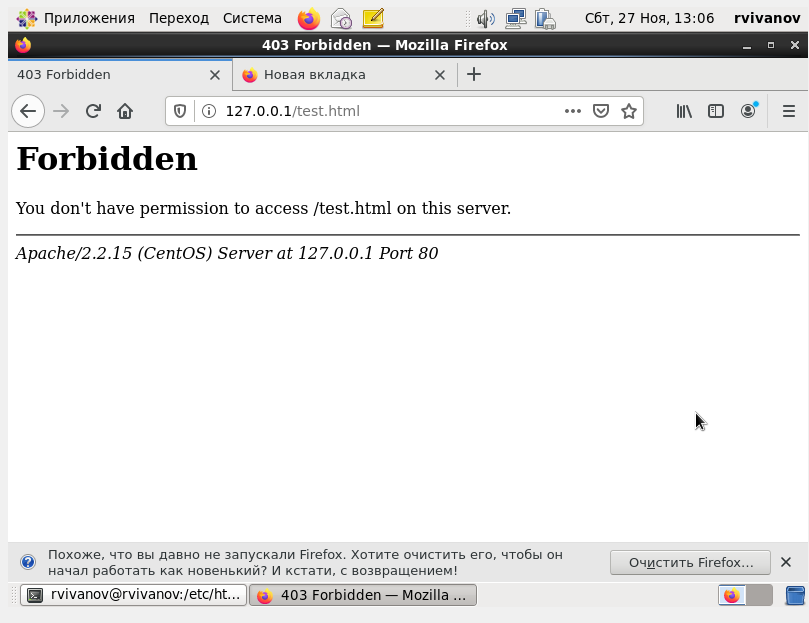
Выяснение контекста файла

Изменил контекст файла с httpd\_sys\_content\_t на samba\_share\_t (рис - @fig:017).



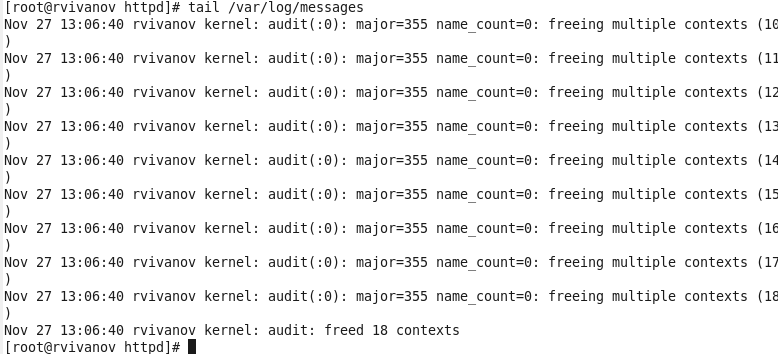
Изменение контекста файла

Попробовал еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес . Получил ошибку (рис - @fig:018).



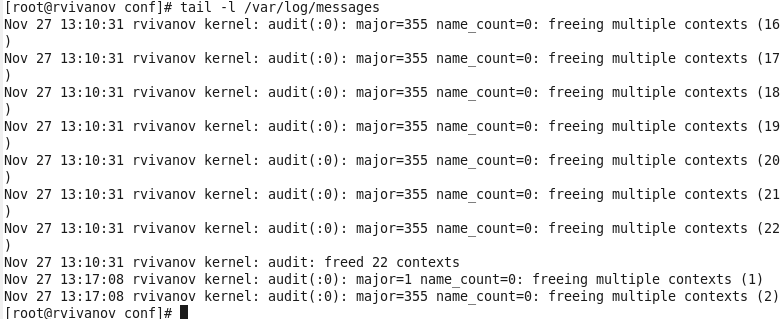
Попытка получить доступ к файлу через веб-сервер

Проанализировал ситуацию. Просмотрел log-файлы веб-сервера Apache, а также посмотрел системный лог-файл с помощью команды (рис - @fig:019).



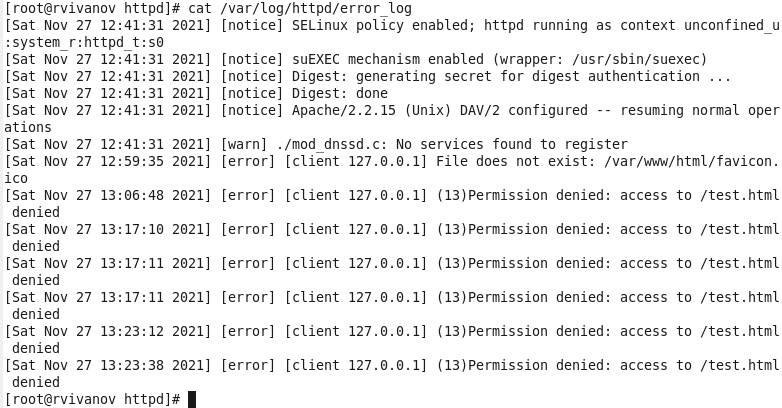
Просмотр системного лог-файла

Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле нашел строчку и заменил ее на (рис - @fig:020).



Изменение строки файла

Просмотрел файл /var/log/http/error\_log (рис - @fig:021).



Просмотр файла /var/log/http/error\_log

Просмотрел файл /var/log/http/access\_log (рис - @fig:022).



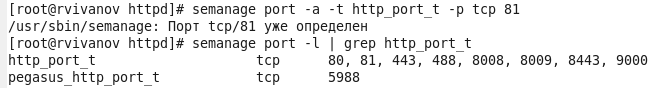
Просмотр файла /var/log/http/access\_log

Просмотрел файл var/log/audit/audit.log (рис - @fig:023).



Просмотр файла /var/log/audit/audit.log

Выполнил команду semanage port -a -t http\_port\_t -p tcp 81. После этого проверил список портов командой semanage port -l | grep http\_port\_t (рис - @fig:024). Убедился, что порт 81 появился в списке.

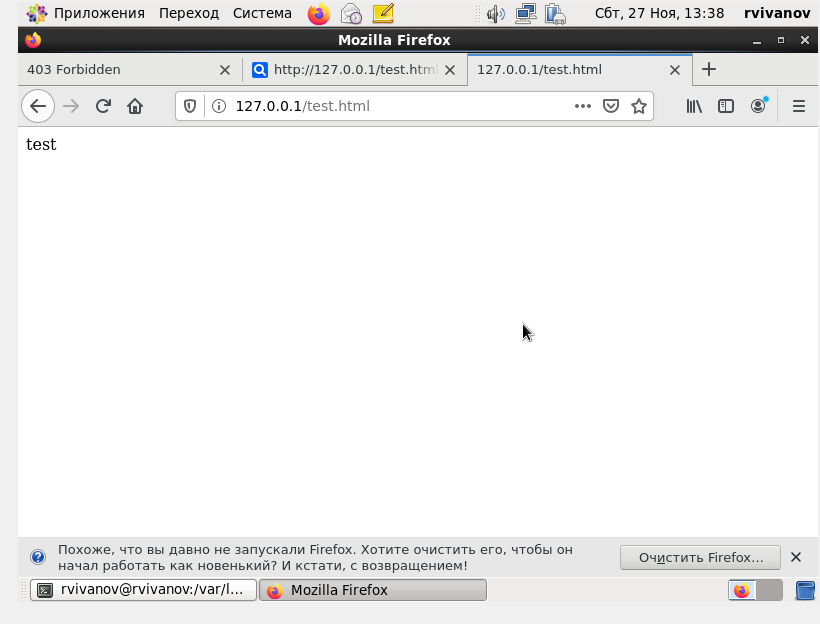


Просмотр портов

Вернул контекст httpd\_sys\_content\_t к файлу с помощью команды chcon -t httpd\_sys\_content\_t /var/www/html/test.html (рис - @fig:025). После этого попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес (рис - @fig:026).

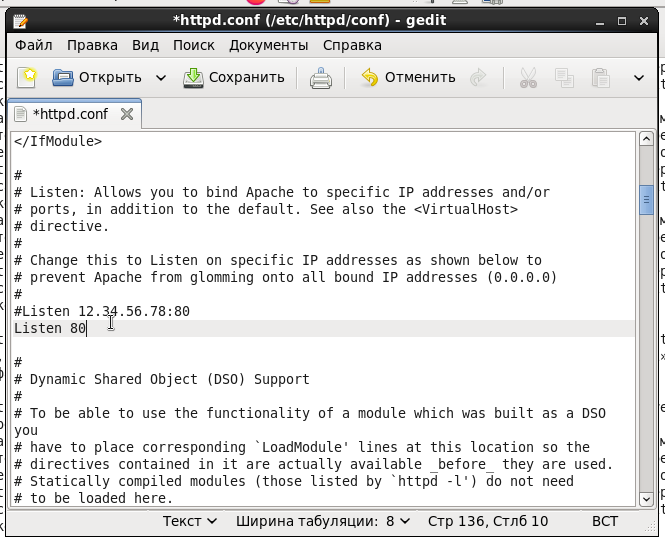
Возвращение исходного контекста

Возвращение исходного контекста



Получение доступа к файлу через веб-сервер

Исправил обратно конфигурационный файл apache, вернув (рис - @fig:027).



Возвращение строки

Попытался удалить привязку http\_port\_t к 81 порту (рис - @fig:028).

Попытка удаления привязки http_port_t к 81 порту

Попытка удаления привязки http\_port\_t к 81 порту

Удалил файл (рис - @fig:029).

Удаление файла 

Удаление файла

# Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux.

Проверил работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 6. Мандатное разграничение прав в Linux.