Лабораторная работа №6

Основы Информационной Безопасности

Чистов Даниил Максимович

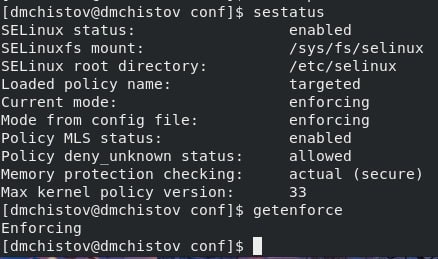
Содержание

# 1 Цель работы

Целью данной лабораторной работы является развитие навыков администрирования ОС Linux, получение первого практического знакомства с технологией SELinux, проверка работы SELinux на практике совместно с веб-сервером Apache.

# 2 Выполнение лабораторной работы

Вхожу в систему, убеждаюсь командой sestatus, что SELinux работает в режиме enforcing политики targeted (рис. **¿fig:001?**).

a

Командой service httpd status убеждаюсь, что веб-сервер Apache работает (рис. 1).

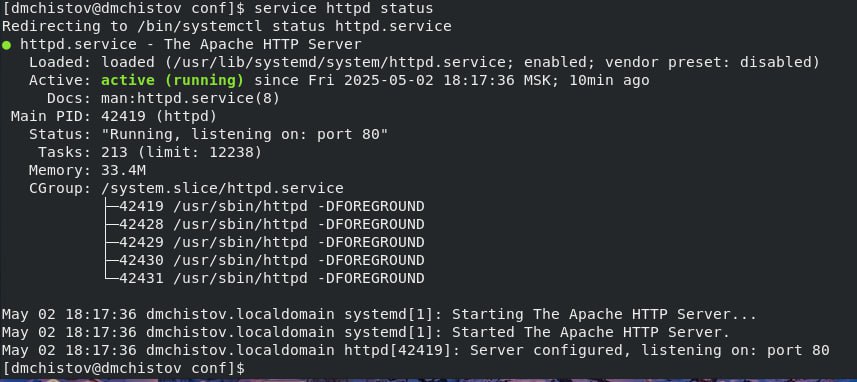


Рис. 1: Вывод команды service httpd status

Командой ps auxZ | grep httpd нахожу процессы веб-сервера Apache и определяю его контекст безопасности - httpd\_t (рис. 2).

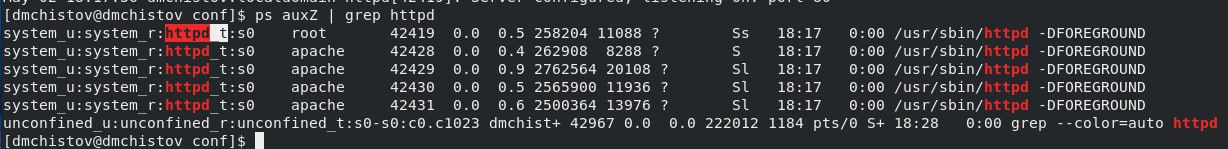


Рис. 2: Процессы Apache

Командой sestatus -b | grep httpd смотрю текущее состояние переключателей SELinux для Apaceh, действительно большинство из них в положении “off” (рис. 3).

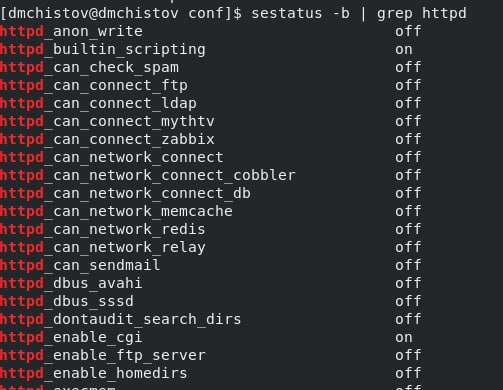


Рис. 3: Состояние переключателей SELinux для Apache

Командой seinfo смотрю статистику по политике - вижу, что типов 5015, пользователей - 8, ролей - 15 (рис. 4).

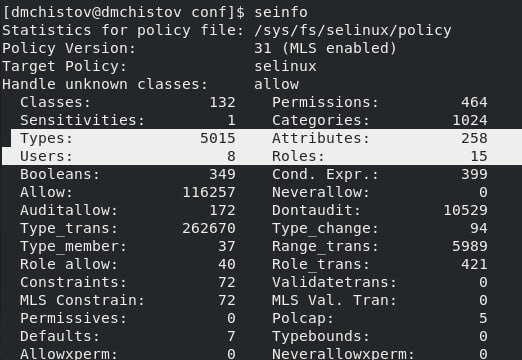


Рис. 4: Статистика по политике

Определяю тип файлов и поддиректорий в /var/www, там лежат файлы Apache типа (рис. 5).

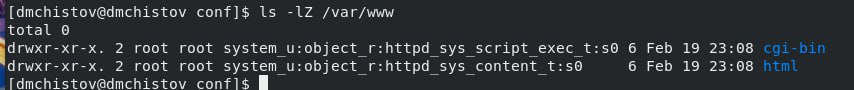


Рис. 5: Типы файлов в /var/www

Определяю тип файлов в /var/www/html - нету никаких файлов, также определяю круг пользователей, которым разрешено создание файлов этой директории - только root пользователь на такое способен (рис. 6).

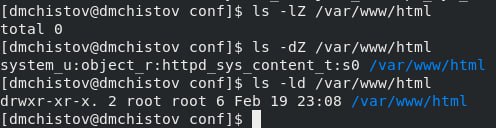


Рис. 6: Данные по /var/www/html

От имени суперпользователя создаю html файл test.html - простая веб-страница с текстом - test (рис. 7).



Рис. 7: test.html

Проверяю созданный мною файл на контекст - httpd - для Apache (рис. 8).



Рис. 8: test.html - контекст

Через браузер захожу на эту веб-страничку и вижу соответствующий текст (рис. 9).

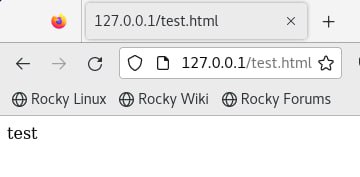


Рис. 9: test.html - в браузере

Командой ls -Z /var/www/html/test.html проверяю контекст этого файла - httpd\_sys\_content\_t (такой тип позволяет httpd получить доступ к файлу, поэтому мы можем его открыть через браузер) с unconfined\_u (свободный пользователей) (рис. 10).

test.html - контекст

Рис. 10: test.html - контекст

Меняю контекст этого файла с httpd\_sys\_content\_t на, например, samra\_share\_t (рис. 11).

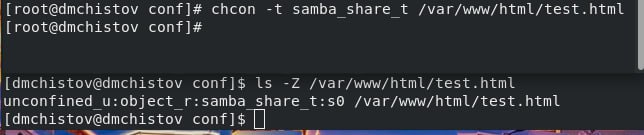


Рис. 11: test.html - новый контекст

Пытаюсь заново обратиться к веб-странице через браузер и получаю отказ (рис. 12).

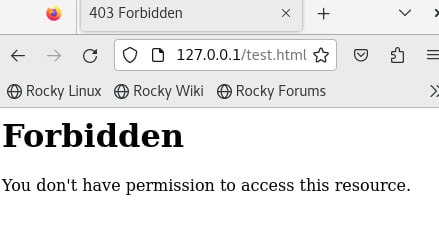


Рис. 12: test.html - отказано в доступе

Смотрю лог файлы сервера Apache и пытаюсь разобраться что не так - думаю, дело в том, что мы поменяли тип файла несколькими шагами ранее. Как минимум в логах нас просят поставить какой-то тип данному файлу (рис. 13).

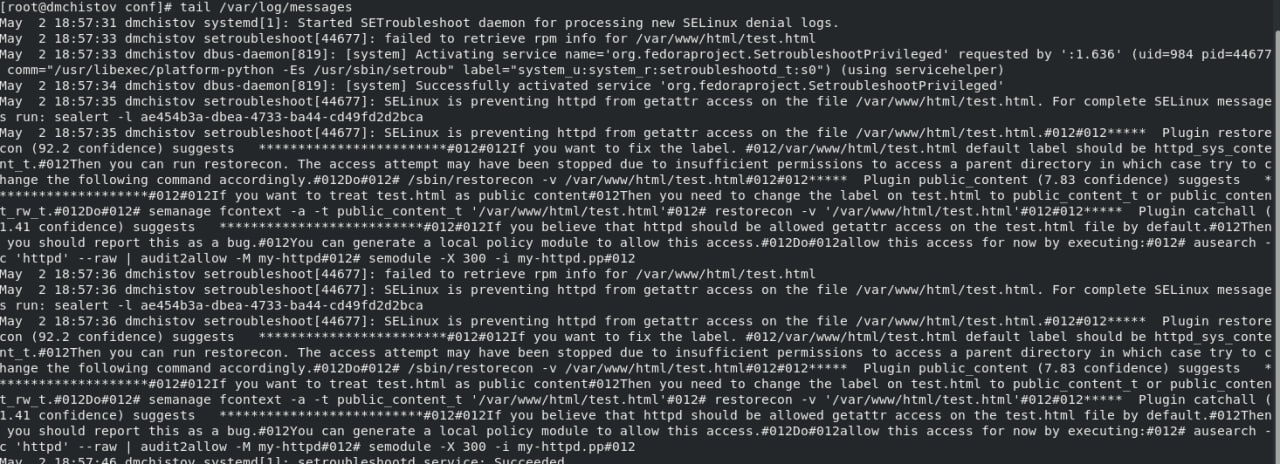


Рис. 13: test.html - расследование причины отказа

Запускаю веб-сервер Apache на прослушивании TCP-порта 81, а не 80 - заменяю строку в конфиг файле веб-сервера (рис. 14).

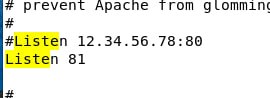


Рис. 14: Веб-сервер на прослушивании порта 81

Теперь после перезапуска мне не просто отказано в доступе, а сама страничка уже не грузится (рис. 15).

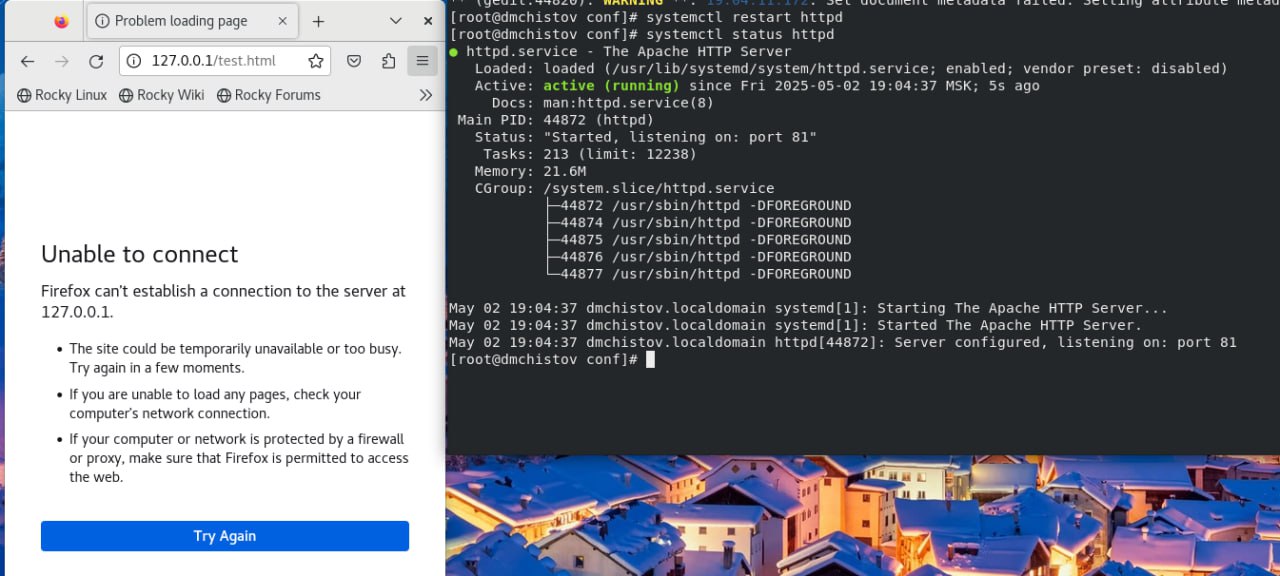


Рис. 15: Веб-сервер не загружает страничку

Смотрю лог файлы - сервер прослушивает порт 81 (рис. 16).

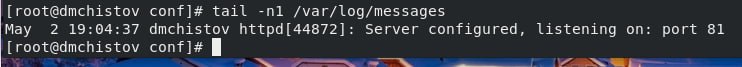


Рис. 16: Расследую ситуацию - прослушивание на порте 81

Смотрю другие лог файлы, вижу, что мне говорят об отсутствии прав (рис. 17).

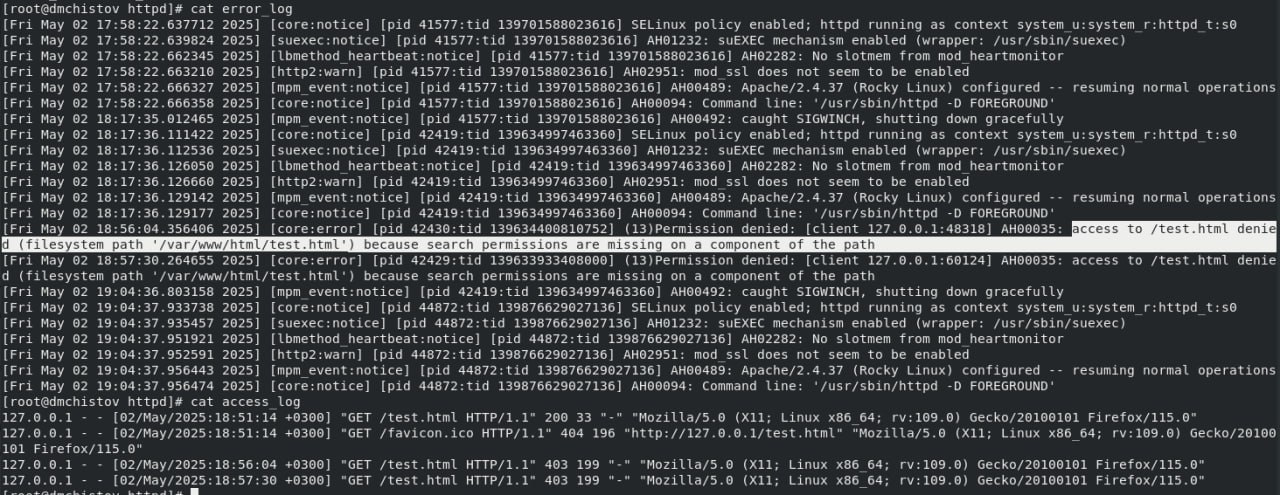


Рис. 17: Расследую ситуацию - отсутствие прав

Командой semanage port -a -t http\_port\_t -p tcp 81 добавляю порт 81, затем смотрю появился ли он - конечно появился (рис. 18).

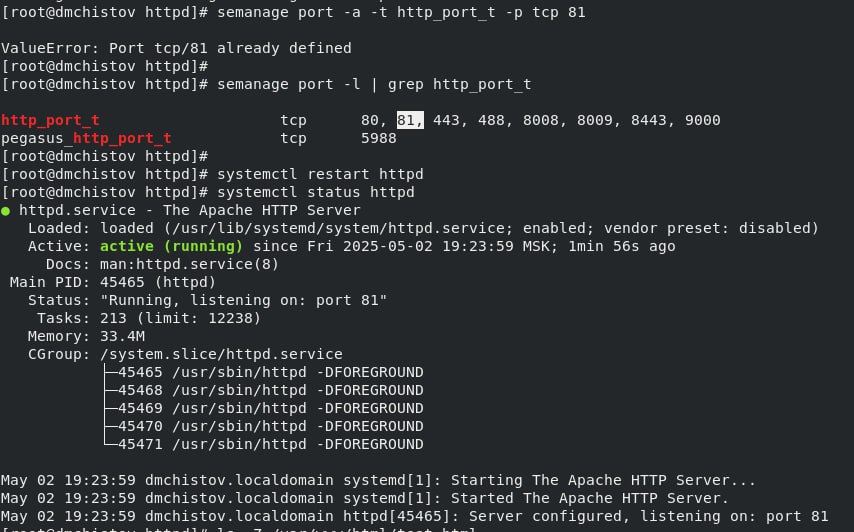


Рис. 18: Новый порт - 81

Перезапускаю веб-сервер Apache - всё успешно, нам нужно было объявить ему о новом порте 81, т.к. его не было в списке, а конфиге мы поставили прослушивание этого на тот момент отсутствующего порта. Затем возвращаю нашей веб-страничке необходимый её тип httpd\_sys\_content\_t и через браузер обращаюсь к той же веб-страничке, но через порт 81 (http://127.0.0.1:81/test.html) - всё работает - текст виден (рис. 19).

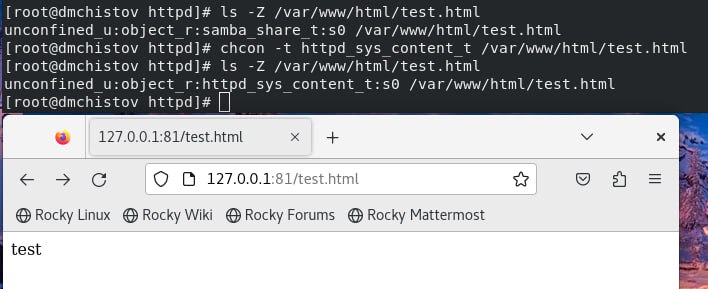


Рис. 19: Сайт открывается на порте 81

Завершаю работу - удаляю привзяку к порту 81, а также удаляю созданный нами файл test.html (рис. 20).

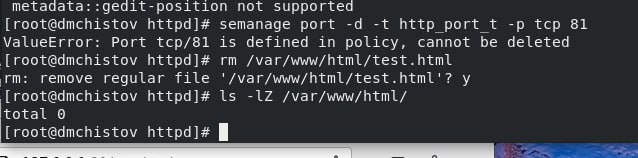


Рис. 20: Завершение работы

# 3 Выводы

В результате выполнения данной лабораторной работы я развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux, проверил работу SELinux на практике совместно с веб-сервером Apache.

# 4 Список литературы

[Лабораторная работа №6](https://esystem.rudn.ru/pluginfile.php/2580600/mod_resource/content/2/006-lab_selinux.pdf)