Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Галацан Николай, НПИбд-01-22

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы [1]

Убеждаюсь, что SELinux работает в режиме enforcing политики targeted. Также убеждаюсь, что веб-сервер запущен и работает (рис. 1).

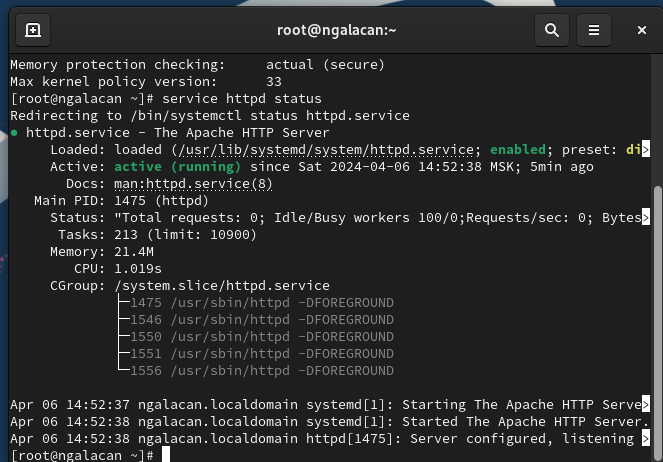


Рис. 1: Режим работы SELinux, статус httpd

Определяю контекст безопасности веб-сервера Apache. Просматриваю текущее состояние переключателей SELinux (рис. 2).

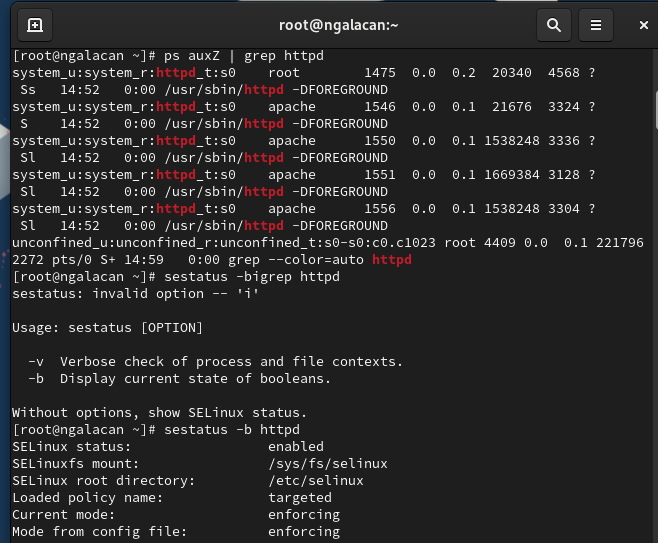


Рис. 2: Контекст безопасности веб-сервера Apache, состояние переключателей SELinux

Просматриваю статистику по политике с помощью команды seinfo (рис. 3).

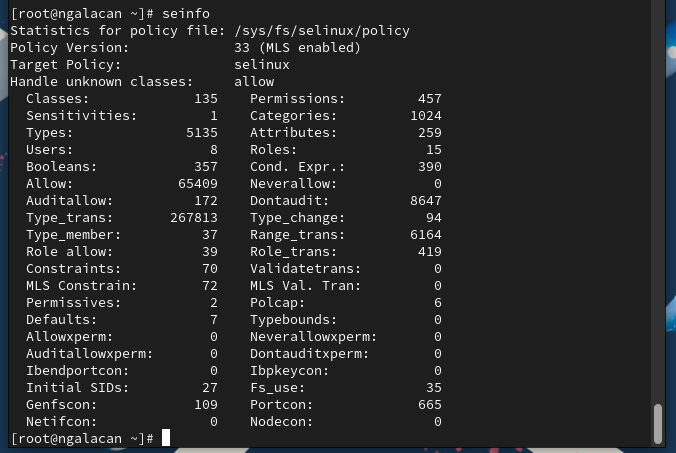


Рис. 3: Статистика по политике

Определяю тип файлов и поддиректорий, находящихся в директории /var/www, /var/www/html, создаю файл test.html следующего содержания:

<html>  
<body>test</body>  
</html>

и проверяю контекст созданного файла (рис. 4).

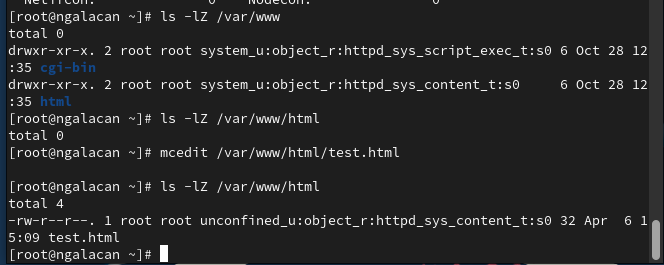


Рис. 4: Просмтр файлов, создание test.html и просмотр контекста

Обращаюсь к файлу через веб-сервер и вижу простую веб-страницу (рис. 5).

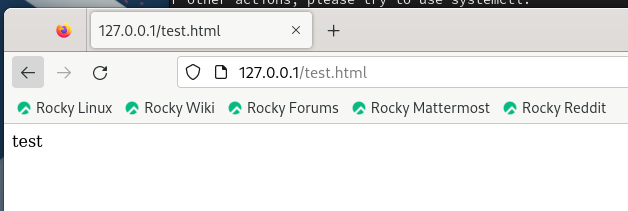


Рис. 5: Запуск файла в браузере

Просматриваю справку по httpd и selinux. Проверяю контекст файла. Тип httpd\_sys\_content\_t позволяет процессу httpd получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер. Меняю контекст файла и проверяю. Пробую еще раз открыть файл в браузере, но файл не отображается по той причине, что httpd не имеет доступа к измененному контексту файла (рис. 6).

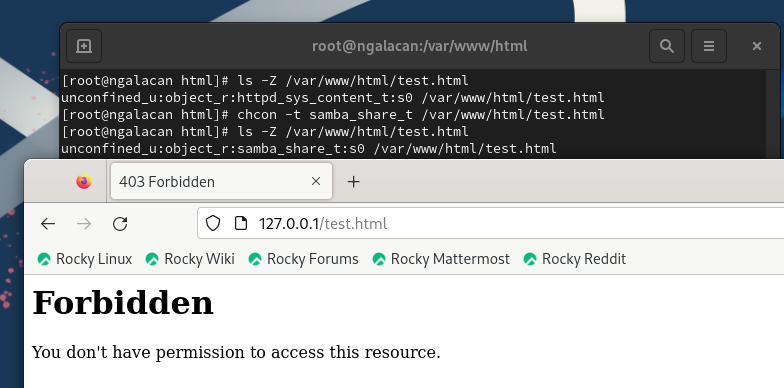


Рис. 6: Изменение контекста файла и попытка просмотра

Просматриваю лог-файлы (рис. 7).

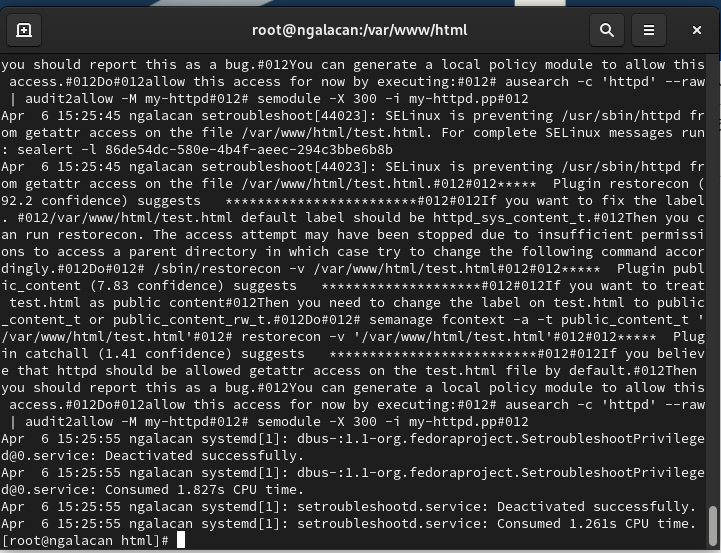


Рис. 7: Просмотр лог-файла

В файле /etc/httpd/conf/httpd.conf меняю порт на 81 (рис. 8).

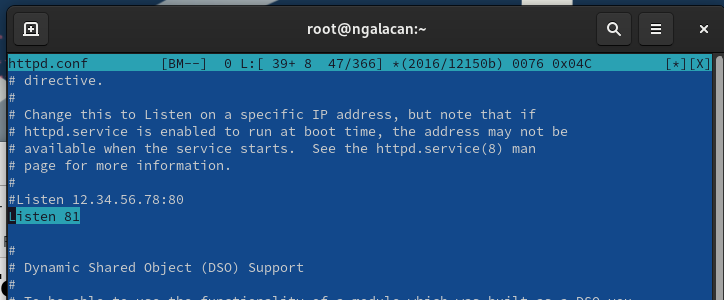


Рис. 8: Изменение порта в конфигурационном файле

Перезагружаю веб-сервер и наблюдаю сбой (рис. 9).

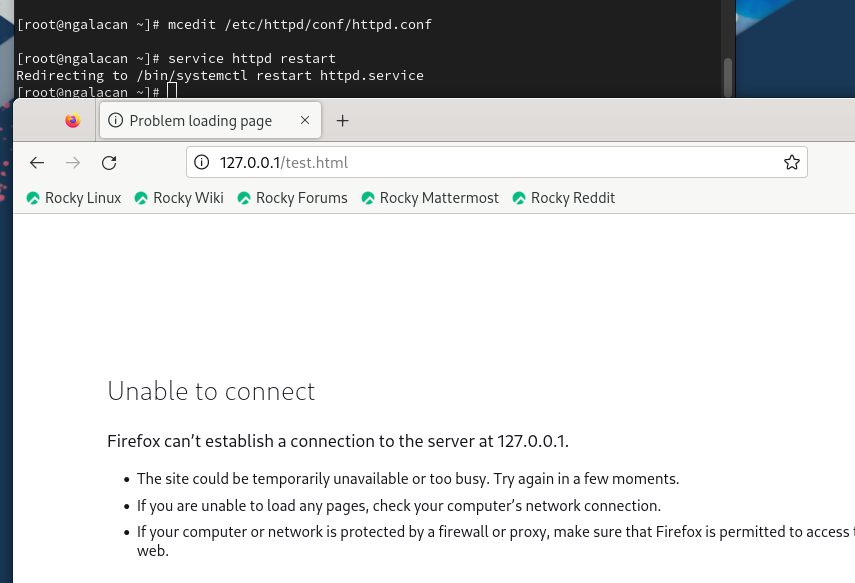


Рис. 9: Сбой веб-сервера

Анализирую лог-файлы (рис. 10).

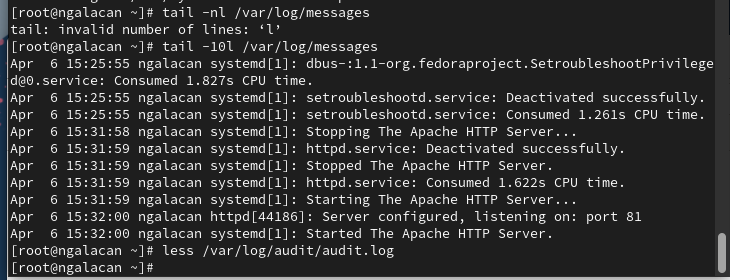


Рис. 10: Просмотр лог-файла

Выполняю команду semanage port -a -t http\_port\_t -р tcp 81 и проверяю список портов командой semanage port -l | grep http\_port\_t и вижу, что порт 81 появился в списке. Перезагружаю веб-сервер. Возвращаю контекст для test.html, к которому httpd имеет доступ (рис. 11).

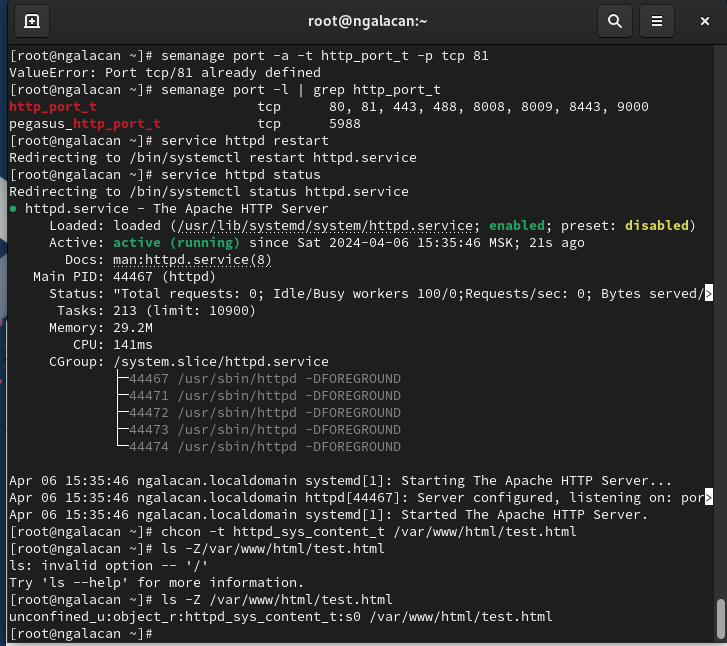


Рис. 11: Добавление порта 81 и проверка. Перезапуск веб-сервера. Возвращение контекста

После этого тестовая страница вновь открывается в браузере.

Исправляю конфигурационный файл обратно, изменив порт на 80. Удаляю привязку http\_port\_t к 81 порту. Удаляю файл /var/www/html/test.html (рис. 12).

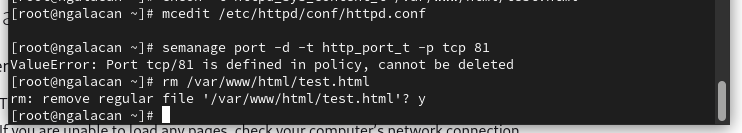


Рис. 12: Завершение выполнения работы

# 3 Выводы

Я развил навыки администрирования ОС Linux, познакомился с технологией SELinux. Проверена работа SELinux на практике совместно с веб-сервером Apache.

# Список литературы

1. Кулябов Д.С., Королькова А.В., Геворкян М.Н. Информационная безопасность компьютерных сетей. Лабораторные работы, учебное пособие. Москва: РУДН, 2015. 64 с.