Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Артамонов Тимофей Евгеньевич

Содержание

# 1 Цель работы

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

# 2 Теоретическое введение

В SELinux права доступа определяются самой системой при помощи специально определённых политик. Политики работают на уровне системных вызовов и применяются самим ядром (но можно реализовать и на уровне приложения). SELinux действует после классической модели безопасности Linux: через SELinux нельзя разрешить то, что запрещено через права доступа пользователей или групп. Политики описываются при помощи специального гибкого языка описания правил доступа. В большинстве случаев правила SELinux «прозрачны» для приложений, и не требуется никакой их модификации. В состав некоторых дистрибутивов входят готовые политики, в которых права могут определяться на основе совпадения типов процесса (субъекта) и файла (объекта) — это основной механизм SELinux. Две других формы контроля доступа — доступ на основе ролей и на основе многоуровневой системы безопасности. [1]

# 3 Выполнение лабораторной работы

Убедимся, что SELinux работает в режиме enforcing политики targeted. (рис. 1)

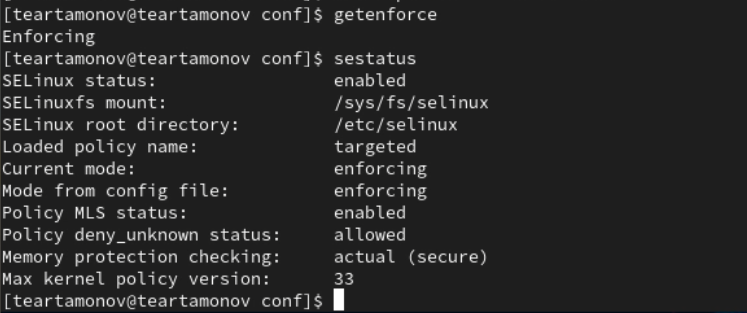


Рис. 1: Все верно

Обратимся к веб-серверу и убедимся, что он работает. (рис. 2)

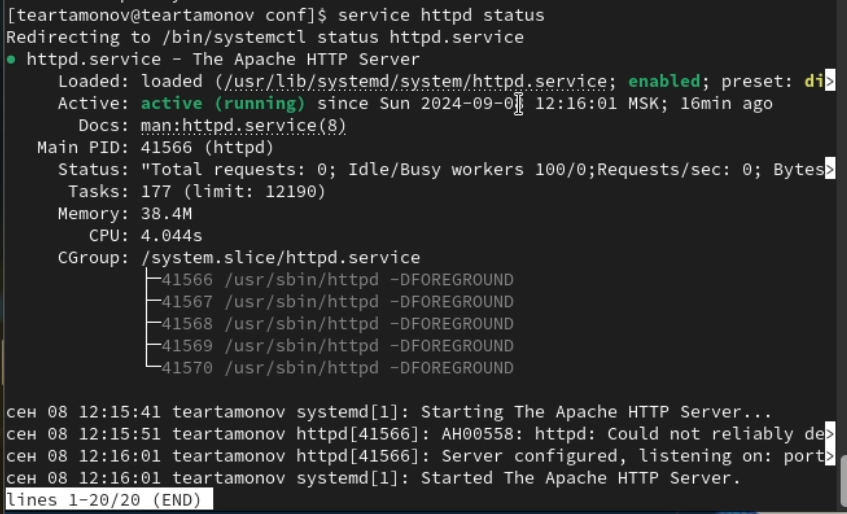


Рис. 2: Веб-сервер работает

Найдем apache в списке процессов. (рис. 3)

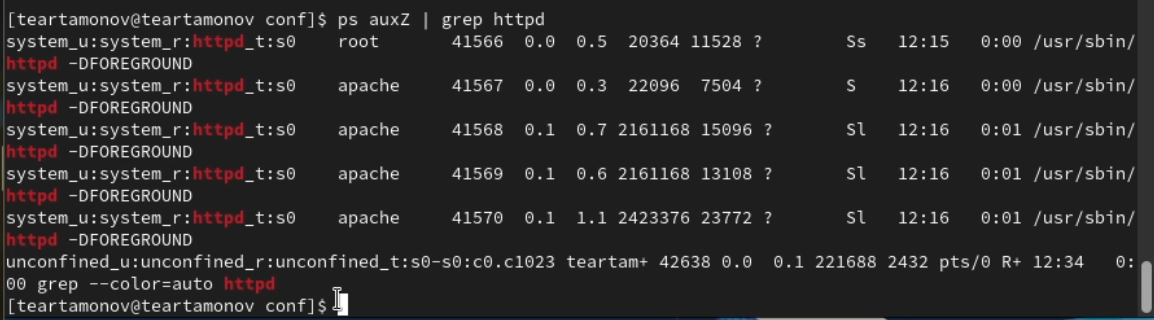


Рис. 3: Нашли с помощью команды ps auxZ | grep httpd

Посмотрим статистику по политике. (рис. 4)

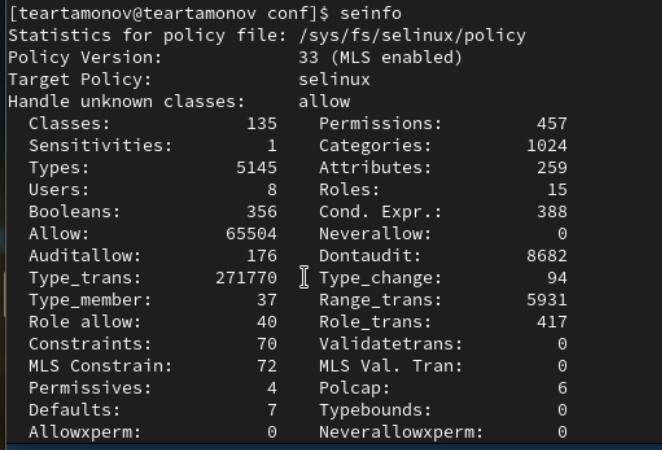


Рис. 4: Видно количество разных сущностей, например, пользователей

Определим тип файлов и директорий в /var/www. (рис. 5)

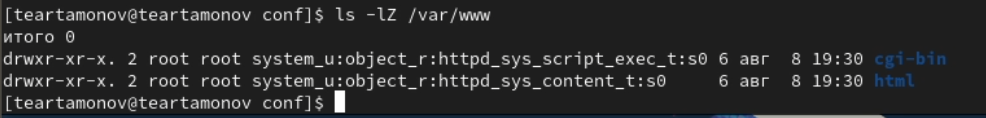


Рис. 5: httpd\_sys\_script\_exec\_t и httpd\_sys\_content\_t

Посмотрим список пользователей. (рис. 6)

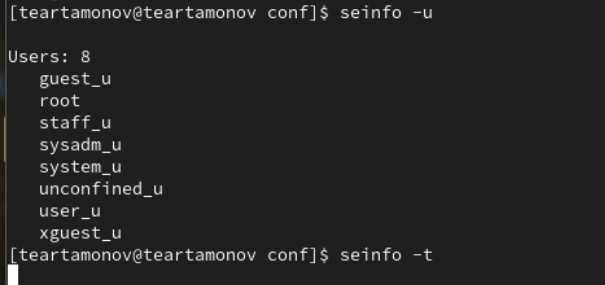


Рис. 6: Список пользователей

Создадим от имени root файл в /var/www/html. (рис. 7)

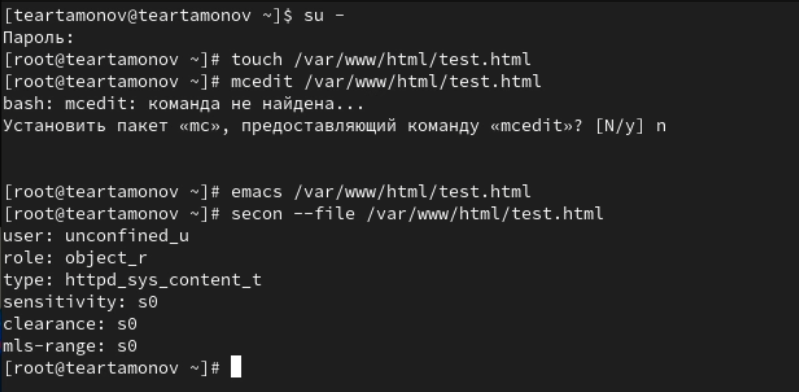


Рис. 7: Успешно

Попробуем посмотреть файл в браузере. (рис. 8)

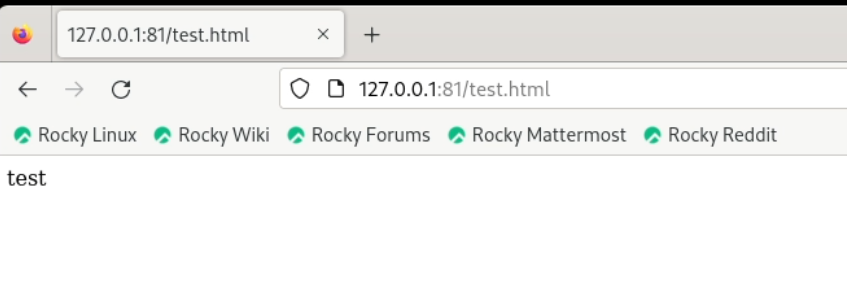


Рис. 8: Успешно

Изменим контекст файла. (рис. 9)

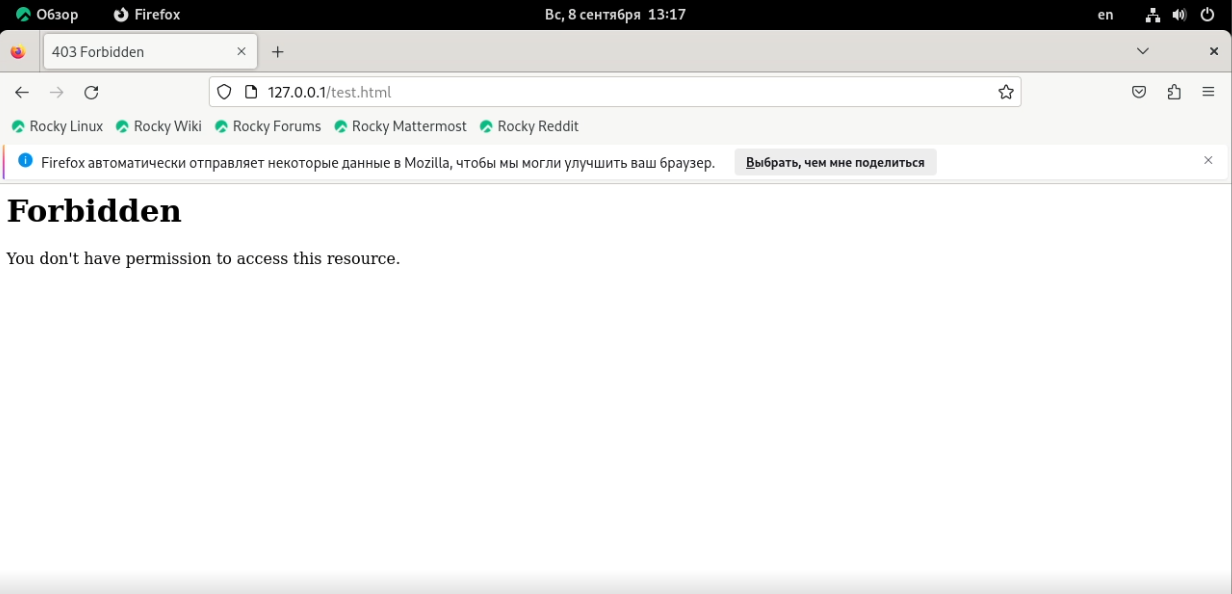


Рис. 9: Успешно, теперь файл не отображается

Добавим на прослушивание порт 81. (рис. 10)

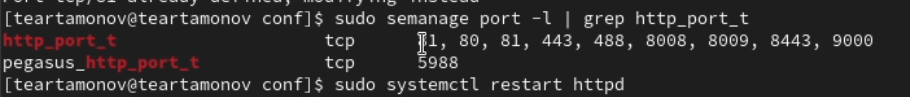


Рис. 10: Успешно, теперь происходит сбой, если не добовать 81 порт в список

Вернем все как было. (рис. 11)

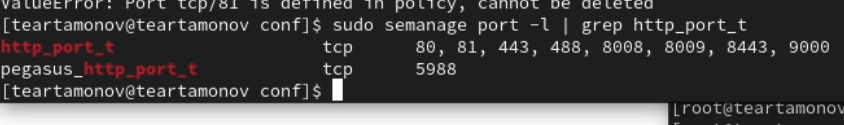


Рис. 11: Успешно

# 4 Выводы

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. SELinux [Электронный ресурс]. Wikimedia Foundation, 2024. URL: <https://ru.wikipedia.org/wiki/SELinux>.