Лабораторная работа №6

Дисциплина: Основы информационной безопасности

Жибицкая Евгения Дмитриевна

Содержание

# 1 Цель работы

Развитие навыков администрирования ОС Linux. Знакомство с технологией SELinux1 и проверка работы SELinx на практике совместно с веб-сервером Аpache.

# 2 Выполнение лабораторной работы

Сначала проведем подготовительные действия: для работы необходим Apache - установим его, также уберем пакетный фильтр (рис. 1).

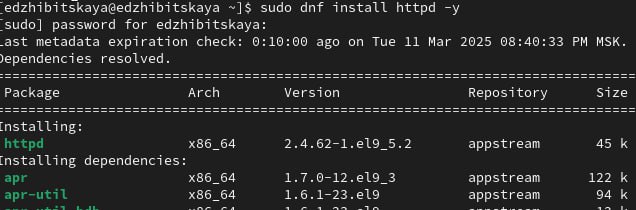


Рис. 1: Установка Apache

Проверим, в каком состоянии находятся службы Selinux и веб-сервер(рис. 2).

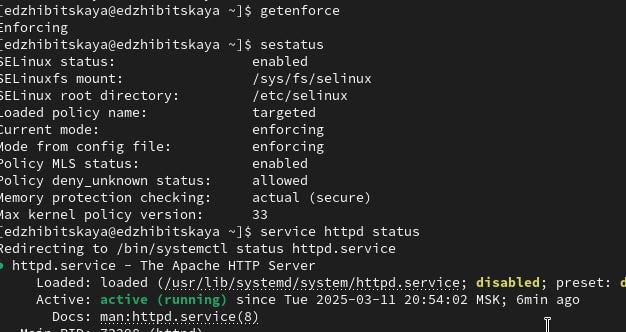


Рис. 2: Статус Selinux

Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности(рис. 3), посмотрим текущее состояние переключателей SELinux для Apache( многие из них выключены)(рис. 4).

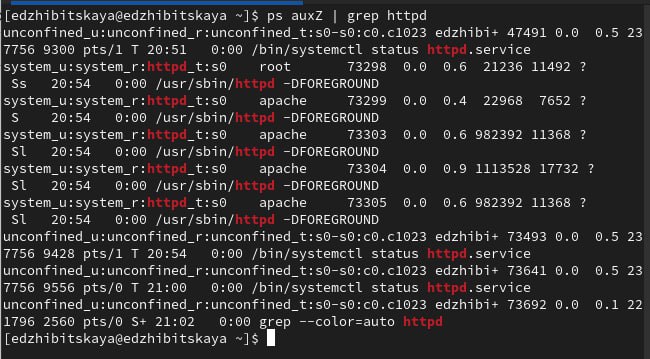


Рис. 3: Контекст безопасности

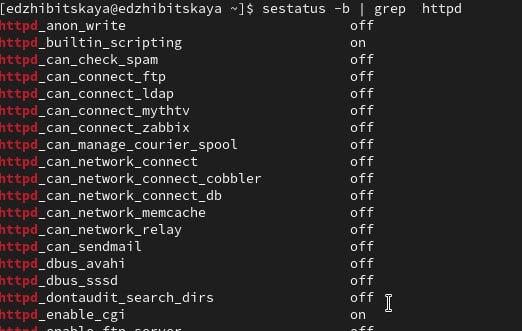


Рис. 4: Состояние переключателей для Apache

Посмотрим статистику по политике с помощью команды seinfo, также определим множество пользователей, ролей, типов(рис. 5).

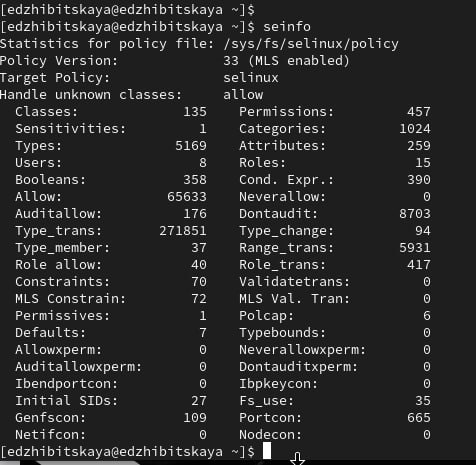


Рис. 5: Статистика

Посмотрим на содержимое каталогов и определим тип файлов(рис. 6).

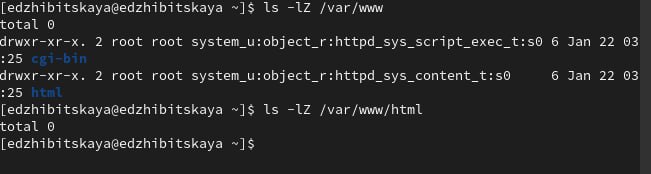


Рис. 6: Типы файлов

От имени администратора создадим файл test.html, добавим туда содержимое(рис. 7) и (рис. 8), перейдем по нужному адресу и посмотрим все ли отображается(рис. 9).



Рис. 7: Создание файла

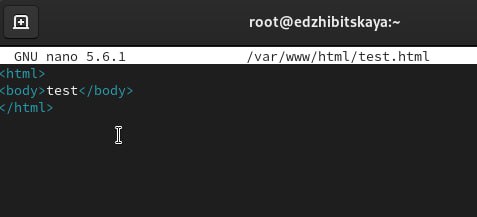


Рис. 8: Test.html

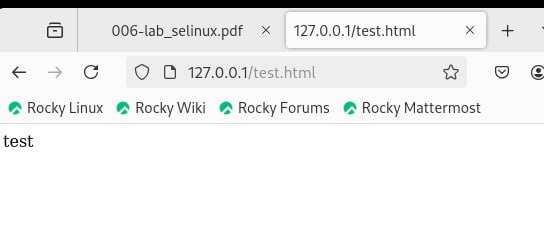


Рис. 9: Проверка сервера

Далее проверим контекст файла командой ls -Z и изучим его подробно. Изменим его на samba\_share\_t и убедимся, что это произошло(рис. 10).

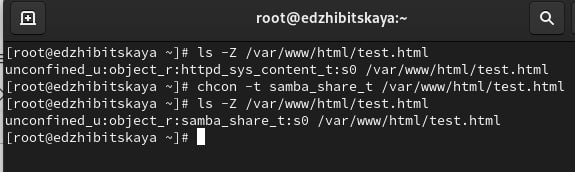


Рис. 10: Контекст файла

Затем еще раз перейдем на веб-сервер - доступа нет(рис. 11).

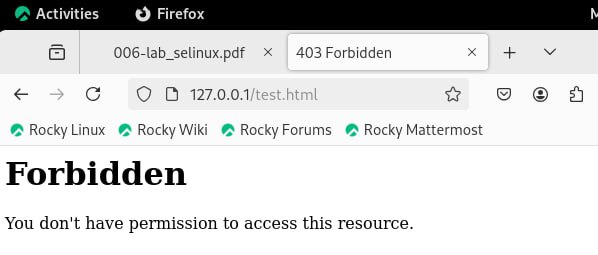


Рис. 11: Доступ к серверу

Просмотрим log-файлы веб-сервера Apache. Также просмотрите системный лог-файл. Если в системе окажутся запущенными процессы setroubleshootd и audtd, то сможем увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log(рис. 12) и (рис. 13).

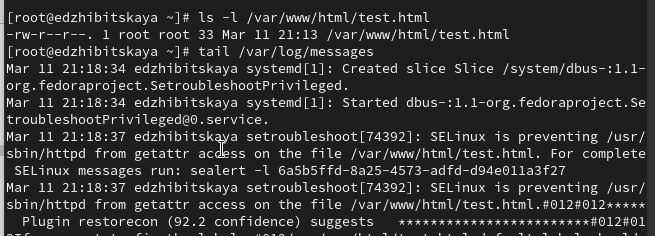


Рис. 12: Системный лог-файл

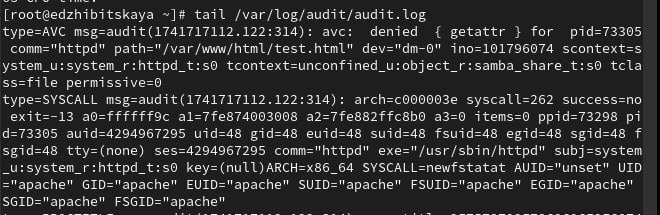


Рис. 13: Доступ к серверу

Попробуем запустить веб-сервер Apache на прослушивание ТСР-порта 81 Для этого в файле /etc/httpd/httpd.conf строчку Listen 80 заменим на Listen 81(рис. 14).

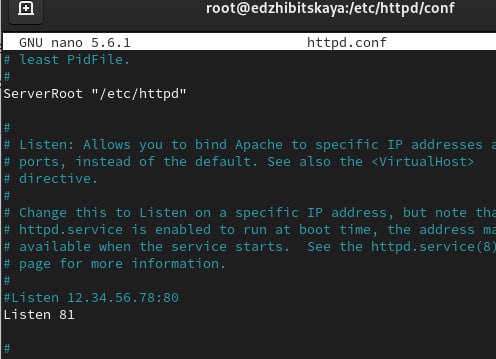


Рис. 14: Порт 81

Перезапустим веб-сервер Apache, проанализируем лог-файлы: /var/log/messages, /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выясним в каких файлах появились записи(рис. 15).

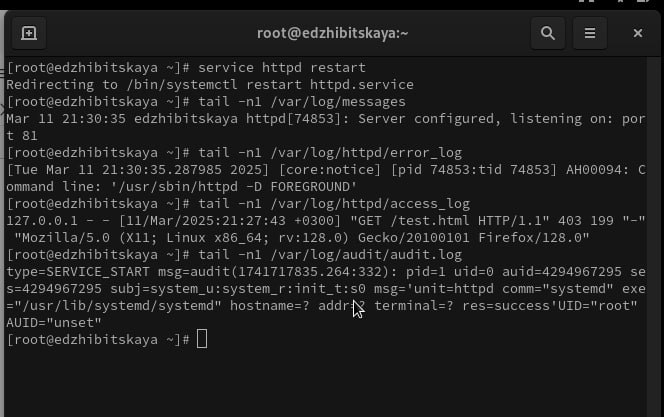


Рис. 15: Перезапуск и анализ файлов

Выполним команду

semanage port -a -t http\_port\_t -р tcp 81

и проверим список портов командой(рис. 16).

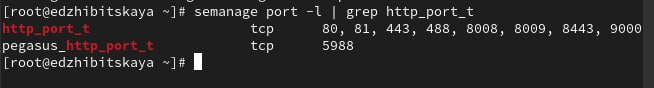


Рис. 16: Системный лог-файл

Попробуем запустить веб-сервер Apache ещё раз.

Вернем контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html и попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html(рис. 17).

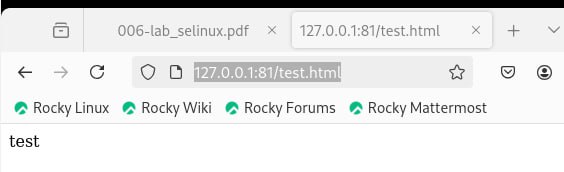


Рис. 17: Повторный запуск сервера

Исправим обратно конфигурационный файл apache, вернув Listen 80(рис. 18), удалим привязку http\_port\_t к 81 порту, удалим файл /var/www/html/test.html(рис. 19).

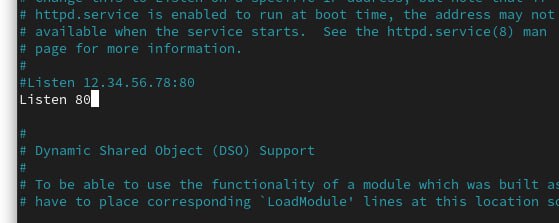


Рис. 18: Возвращение порта 80



Рис. 19: Удаление файла

# 3 Выводы

В ходе работы было произведено знакомство с Apache и Selinux, получены навыки по работе с ними и взаимодействию с веб-сервером

# Список литературы

[ТУИС](https://esystem.rudn.ru/pluginfile.php/2580986/mod_resource/content/2/006-lab_selinux.pdf)