Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Исаханян Эдуард Тигранович

2022 Sep 21th

Содержание

# Цель работы

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

# Выполнение лабораторной работы

## Подготовка лабораторного стенда

В конфигурационном файле /etc/httpd/httpd.conf зададим параметр ServerName. (рис. 1)

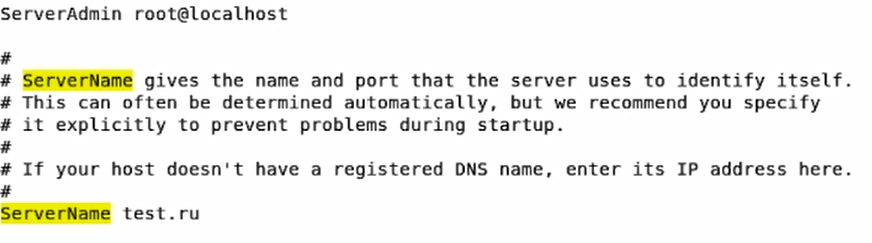


Figure 1: Параметр ServerName

Также проследим, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключим фильтр и добавим разрешающие правила. (рис. 2 - 3)

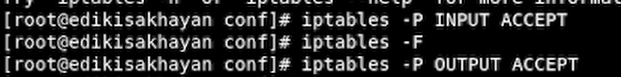


Figure 2: Отключение фильтра

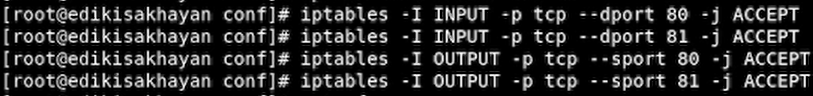


Figure 3: Отключение фильтра

## Выполнение лабораторной работы

Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted. (рис. 4)

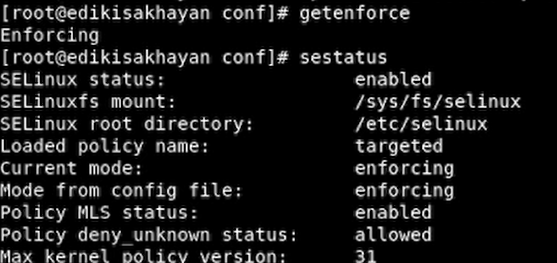


Figure 4: Проверка режима и политики

Обратимся с помощью браузера к веб-серверу, запущенному на компьютере, и убедимся, что последний работает. (рис. 5 - 6)

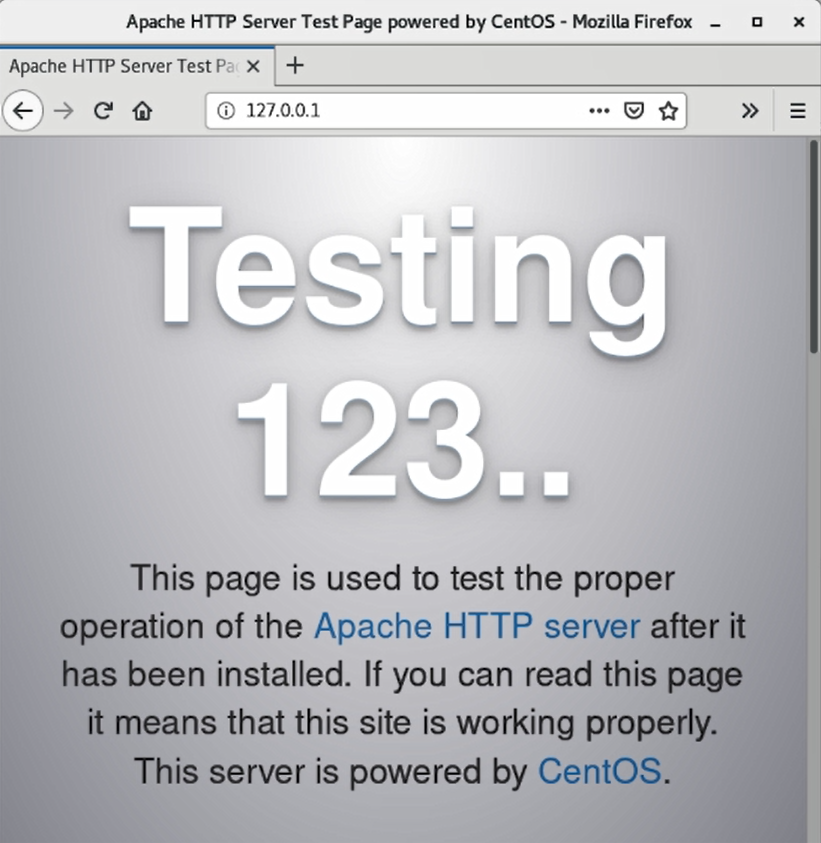


Figure 5: Проверка через браузер

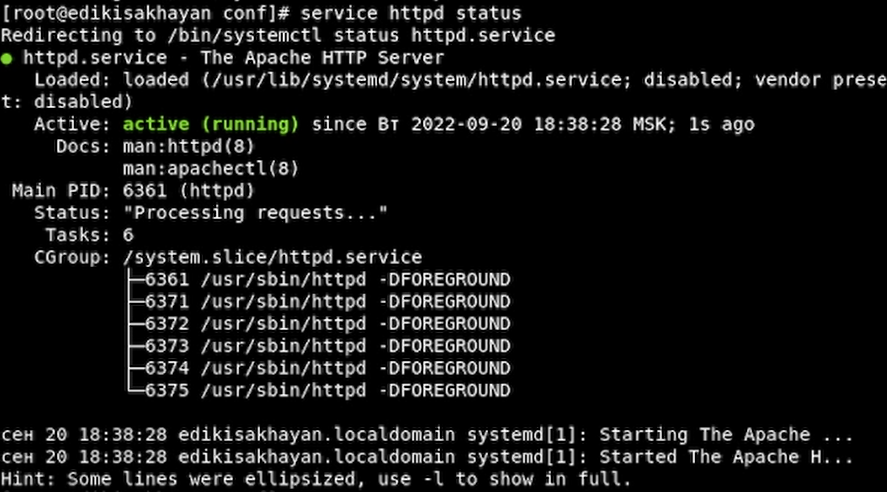


Figure 6: Проверка статуса

Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности. (рис. 7)

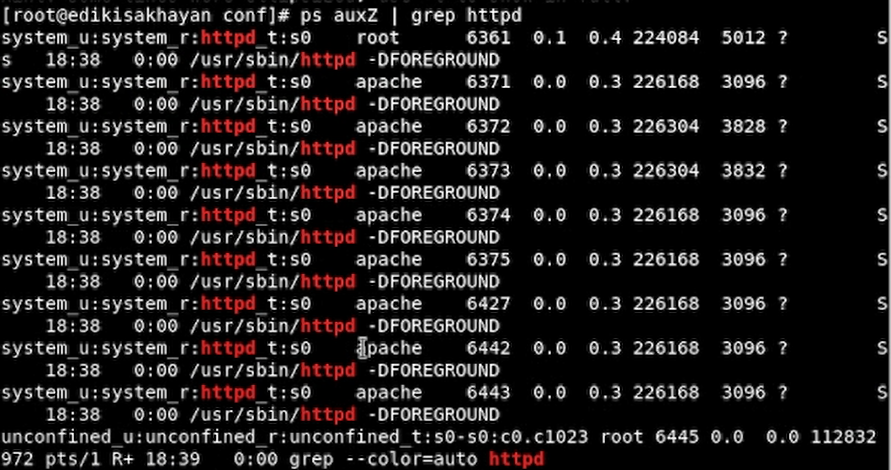


Figure 7: веб-сервер Apache

Посмотрем текущее состояние переключателей SELinux для Apache. (рис. 8)

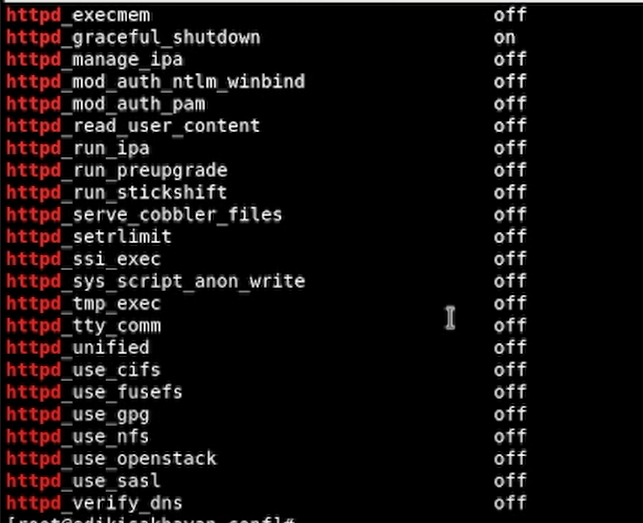


Figure 8: Просмотр переключателей SELinux для Apache

Посмотрем статистику по политике, также определил множество пользователей(8), ролей(14), типов(4793). (рис. 9)

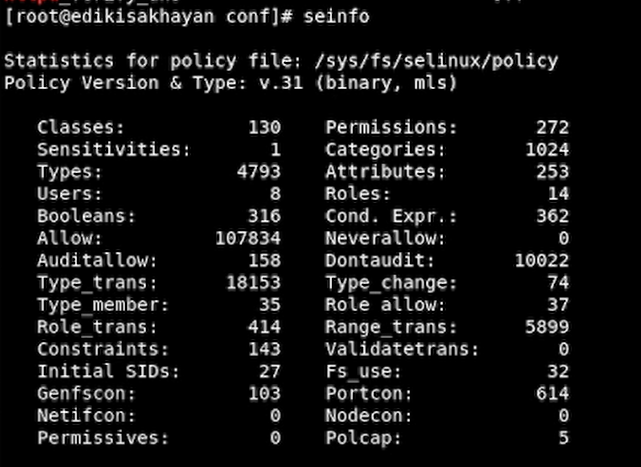


Figure 9: Статистика

Определим тип файлов и поддиректорий, находящихся в директории /var/www, также определим тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html, и ппределим круг пользователей, которым разрешено создание файлов в директории /var/www/html. (рис. 10)

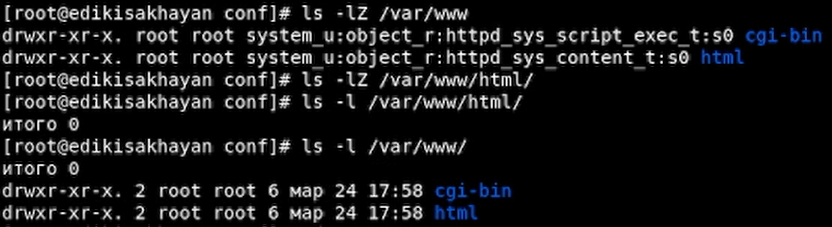


Figure 10: Определение типов файлов и круг пользователей

Создадим от имени суперпользователя html-файл /var/www/html/test.html. (рис. 11)

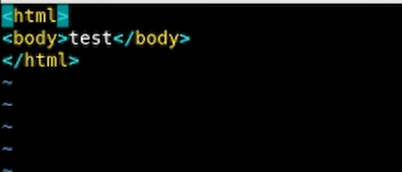


Figure 11: Создание файла

Проверим контекст созданного файла: httpd\_sys\_content\_t. (рис. 12)

Figure 12: Проверка

Figure 12: Проверка

Обратимся к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедимся, что файл был успешно отображён. (рис. 13)

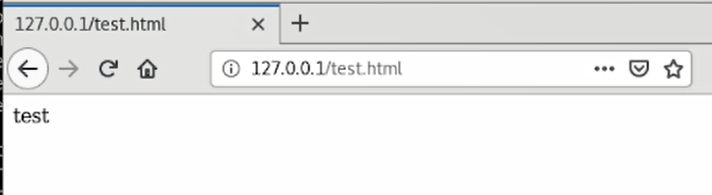


Figure 13: Получение доступа к файлу через браузер

Проверим контекст файла и изменим контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t. После этого проверим, что контекст поменялся. (рис. 14)

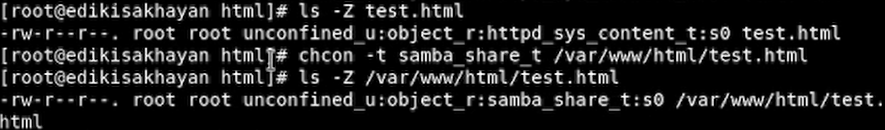


Figure 14: Изменение контекста, проверка

Попробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получим сообщение об ошибке. (рис. 15)



Figure 15: Получение доступа к файлу через браузер

Файл не был отображён потому что мы изменили контекст файла. Просмотрем log-файлы веб-сервера Apache. Также просмотрем системный лог-файл: tail /var/log/messages. (рис. 16)

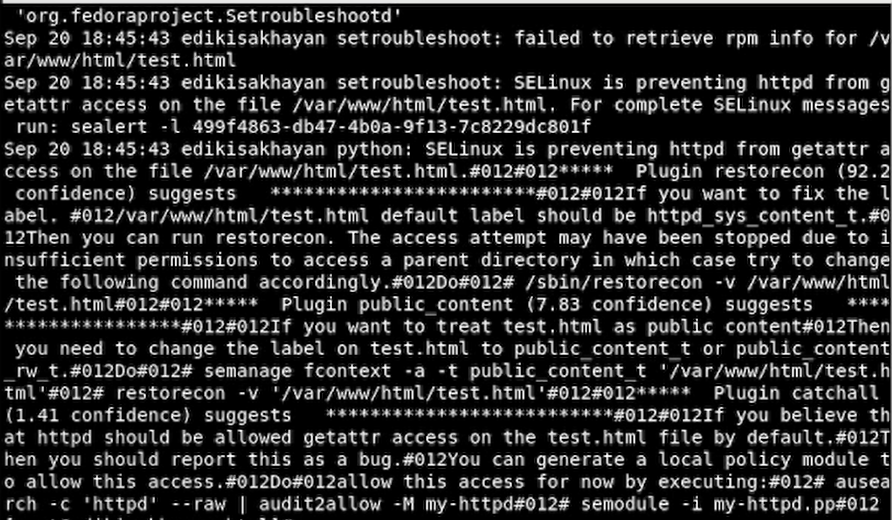


Figure 16: Анализ ситуации

Попробуем запустить веб-сервер Apache на прослушивание ТСР-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдем строчку Listen 80 и заменим её на Listen 81. (рис. 17)

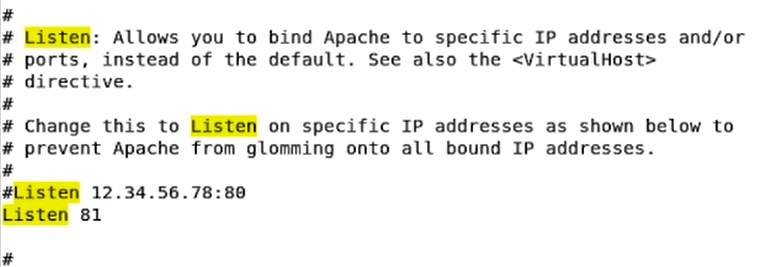


Figure 17: Изменеие порта 80 на 81

Просмотрем файл /var/log/http/error\_log. (рис. 18)



Figure 18: Анализ и просмотр лог-файлов

Выполним команду: semanage port -a -t http\_port\_t -р tcp 81. После этого проверим список портов. Убедимся, что порт 81 появился в списке. (рис. 19)

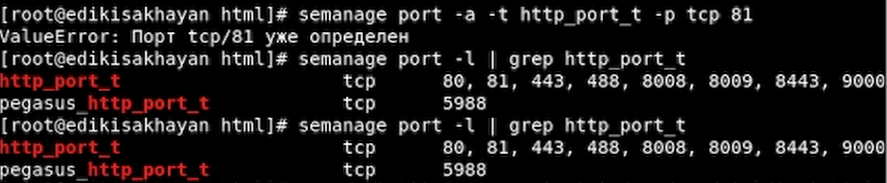


Figure 19: Выполнение и проверка

Вернем контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/test.html. После этого попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Снова увидим содержимое файла — слово «test». (рис. 20 - 21)

Figure 20: Возвращение контекста

Figure 20: Возвращение контекста

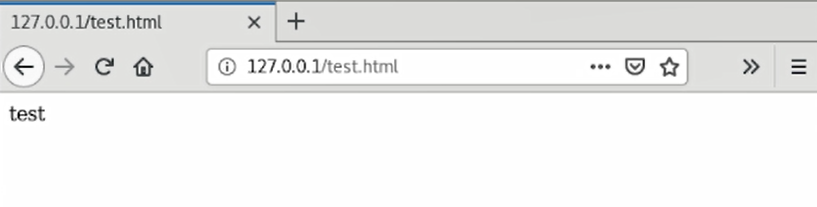


Figure 21: Получение доступа к файлу через браузер

Исправим обратно конфигурационный файл apache, вернув Listen80. (рис. 22)

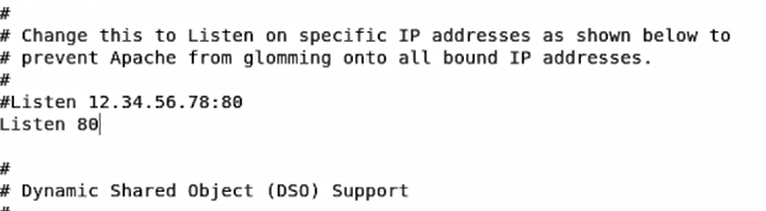


Figure 22: Исправленный файл apache

Удалим привязку http\_port\_t к 81 порту и удалим файл /var/www/html/test.html. (рис. 23)

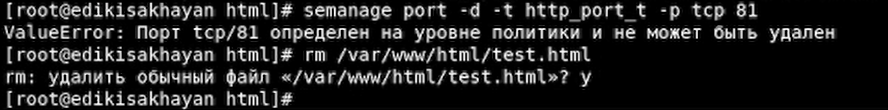


Figure 23: Удаление привязки к 81 порту и удаление файла

# Выводы

Входе работы, мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН” https://esystem.rudn.ru/  
   ::: {#refs} :::