Лабораторная работа № 6

Мандатное разграничение прав в Linux

Беличева Дарья Михайловна

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.

# 2 Теоретическое введение

SELinux (англ. Security-Enhanced Linux — Linux с улучшенной безопасностью) — реализация системы мандатного управления доступа, которая может работать параллельно с классической избирательной системой контроля доступа[1].

Домен – список действий, которые может выполнять процесс. Обычно в качестве домена определяется минимально-возможный набор действий, при помощи которых процесс способен функционировать. Таким образом, если процесс дискредитирован, злоумышленнику не удастся нанести большого вреда.

Роль – список доменов, которые могут быть применены. Если какого-то домена нет в списке доменов какой-то роли, то действия из этого домена не могут быть применены.

Тип – набор действий, которые допустимы по отношения к объекту. Тип отличается от домена тем, что он может применяться к пайпам, каталогам и файлам, в то время как домен применяется к процессам.

Контекст безопасности – все атрибуты SELinux — роли, типы и домены.

# 3 Выполнение лабораторной работы

Подготовим лабораторный стенд: установим веб-сервер Apache, а в конфигурационном файле /etc/httpd/httpd.conf зададим параметр ServerName (рис. 1).

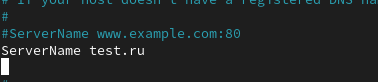


Рис. 1: Задание параметра ServerName

Далее отключим пакетный фильтр (рис. 2).

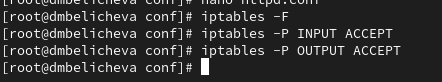


Рис. 2: Отключение пакетного фильтра

Войдем в систему с полученными учётными данными и убедитимся, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.

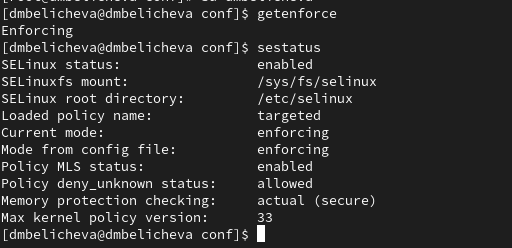


Рис. 3: Проверка режима работы SELinux

Обратимся с помощью браузера к веб-серверу, запущенному на нашем компьютере, и убедимся, что последний работает(рис. 4).

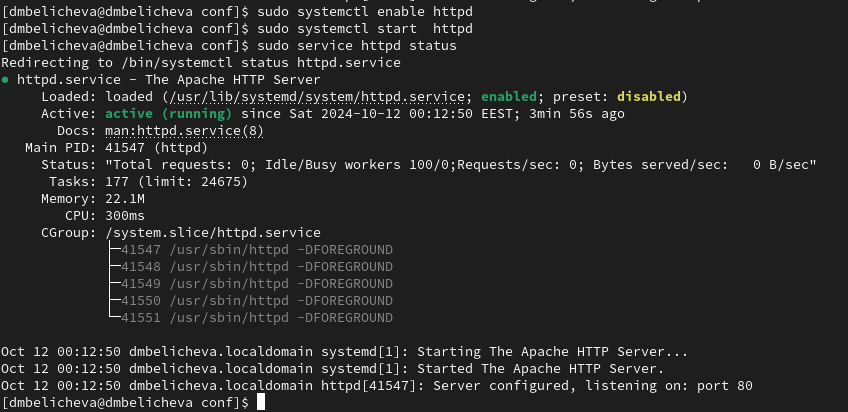


Рис. 4: Проверка статуса веб-сервера

Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности (рис. 5). Информация о контексте находится в первом столбце.

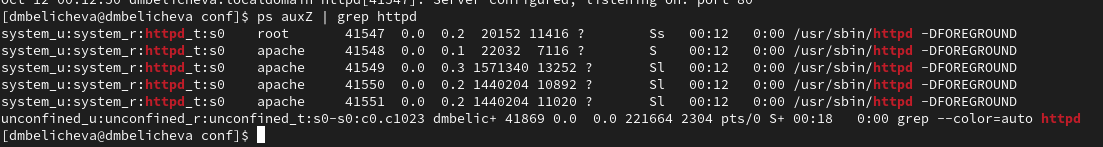


Рис. 5: Контекст безопасности Apache

Посмотрим текущее состояние переключателей SELinux для Apache с помощью команды (рис. 6).

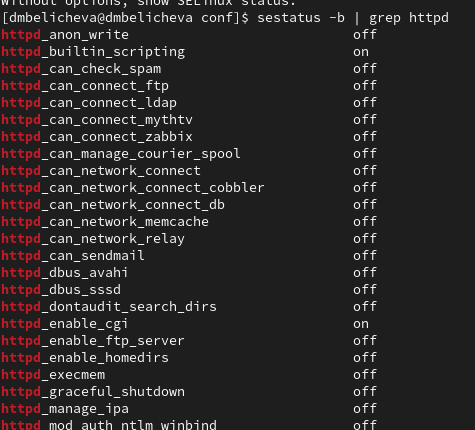


Рис. 6: Текущее состояние переключателей SELinux для Apache

Посмотрим статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов (рис. 7;8).

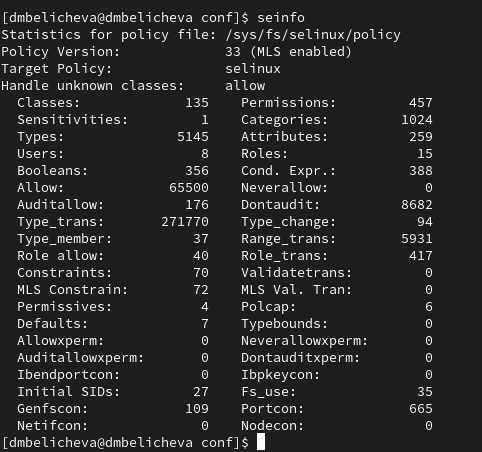


Рис. 7: Статистика по политике

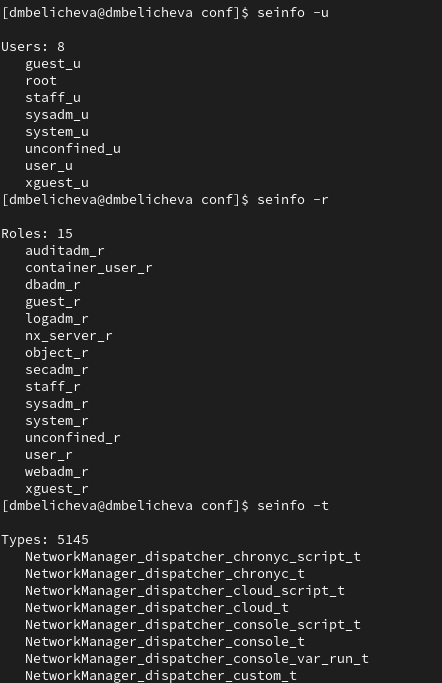


Рис. 8: Множество пользователей, ролей, типов

Определите тип файлов и поддиректорий, находящихся в директории /var/www (рис. 9). Увидим, что есть директория, содержащая cgi-скрипты, и директория /var/www/html, содержащая все скрипты httpd(в данный момент пустая).

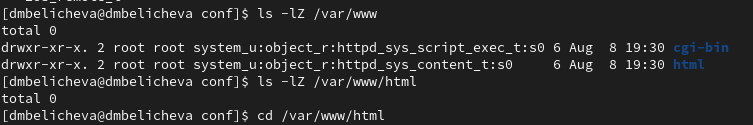


Рис. 9: Просмотр типов директорий в /var/www

Создадим от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания (рис. 10).

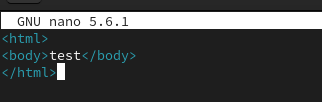


Рис. 10: Содержимое файла /var/www/html/test.html

Проверим контекст созданного вами файла, который был задан по умолчанию этому файлу (рис. 11). Увидим, что файлам по умолчанию сопоставляется свободный пользователь SELinux unconfined\_u, указана роль object\_r используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах и тип httpd\_sys\_content\_t, который позволяет процессу httpd получить доступ к файлу.

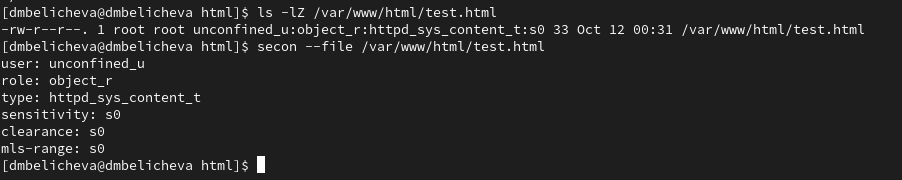


Рис. 11: Проверка контекста файла

Обратимся к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедимся, что файл успешно отображается (рис. 12).

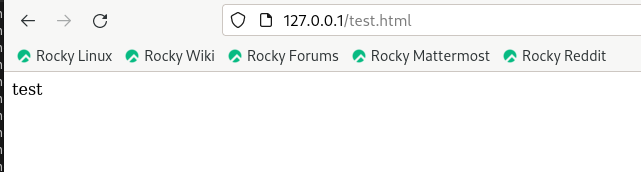


Рис. 12: Запуск файла через веб-браузер

Изучив справку man httpd\_selinux, выясним, какие контексты файлов определены для httpd. Сопоставив их с типом файла test.html увидим, что его контекст httpd\_sys\_content\_t для содержимого, которое должно быть доступно для всех скриптов httpd и для самого демона.

Изменим контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на тот, к которому процесс httpd не должен иметь доступа – samba\_share\_t (рис. 13).



Рис. 13: Изменение контекста файла /var/www/html/test.html

Теперь снова попробуем получить доступ к файлу через браузер и получим отказ (рис. 14).

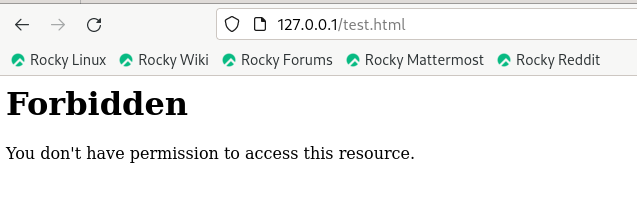


Рис. 14: Отказ в доступе к html-странице через браузер

Посмотрим log-файлы веб-сервера Apache и системный лог-файл и увидим, что отказ происходит, так как доступ запрещен SELinux именно к веб-серверу(на просто просмотр текстовых файлов это не влияет) (рис. 15).

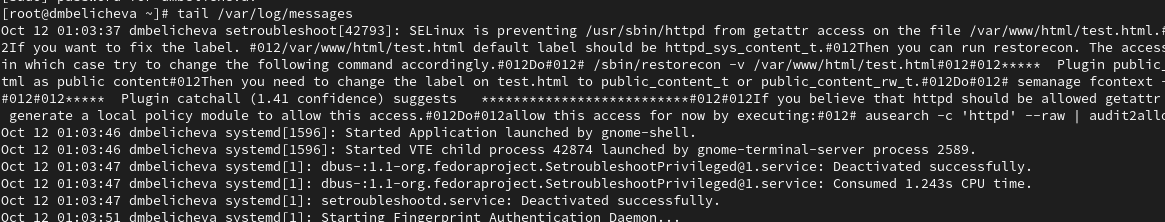


Рис. 15: Просмотр log-файлов веб-сервера Apache

Запустим веб-сервер Apache на прослушивание ТСР-порта 81. Для этого в файле /etc/httpd/httpd.conf найдем строчку Listen 80 и заменим её на Listen 81 (рис. 16).

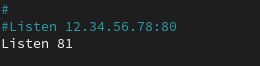


Рис. 16: Замена прослушиваемого порта

Выполним перезапуск веб-сервера Apache. Произошёл сбой, потому что порт 80 для локальной сети, а 81 нет (рис. 17).

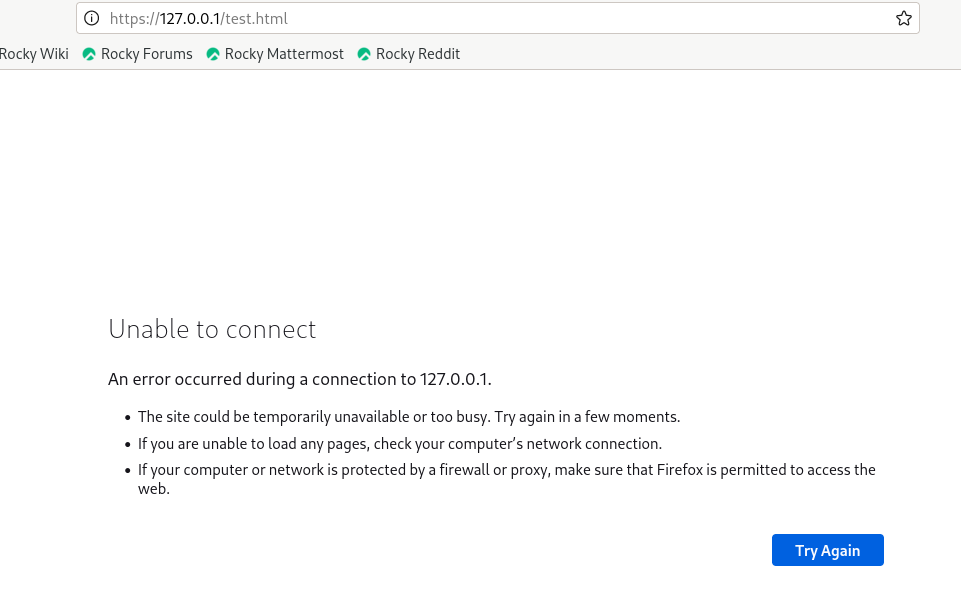


Рис. 17: Открытие html-страницы через браузер при прослушивании 81 порта

В логах можно увидеть запуск сервера через порт 81 (рис. 18).

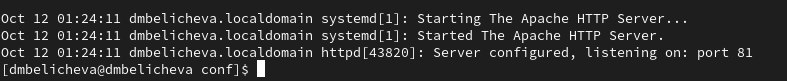


Рис. 18: Проверка запуска сервера через порт 81

Проверим какие порты у нас добавлены в semanage (рис. 19).



Рис. 19: Список портов в semanage

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

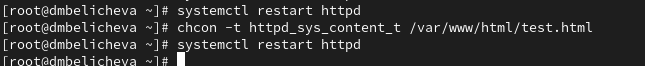


Рис. 20: Возвращение прежнего контекста файла

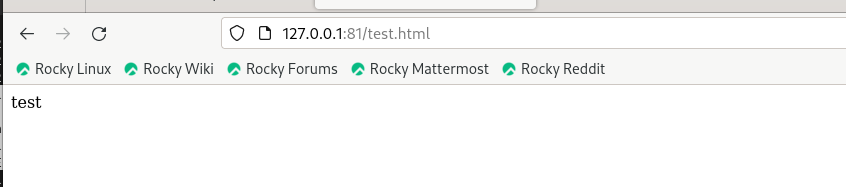


Рис. 21: Открытие html-страницы через браузер

Исправим обратно конфигурационный файл apache, вернув Listen 80. Удалим привязку http\_port\_t к 81 порту. Удалим файл /var/www/html/test.html:

# 4 Выводы

В результате выполнения данной лабораторной работы мною были развиты навыки администрирования ОС Linux, получено первое практическое знакомство с технологией SELinux, а также проверена работа SELinx на практике совместно с веб-сервером Apache.

# Список литературы

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