Лабораторная работа № 6

Мандатное разграничение прав в Linux

Казакова Виктория Алексеевна

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 Ход работы

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted (рис. [1](#fig:001)).

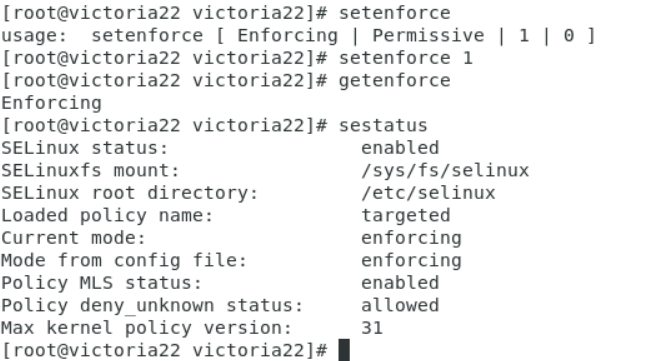


Figure 1: Конфигурация SELinux

1. Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что он работает (рис. [2](#fig:002)).

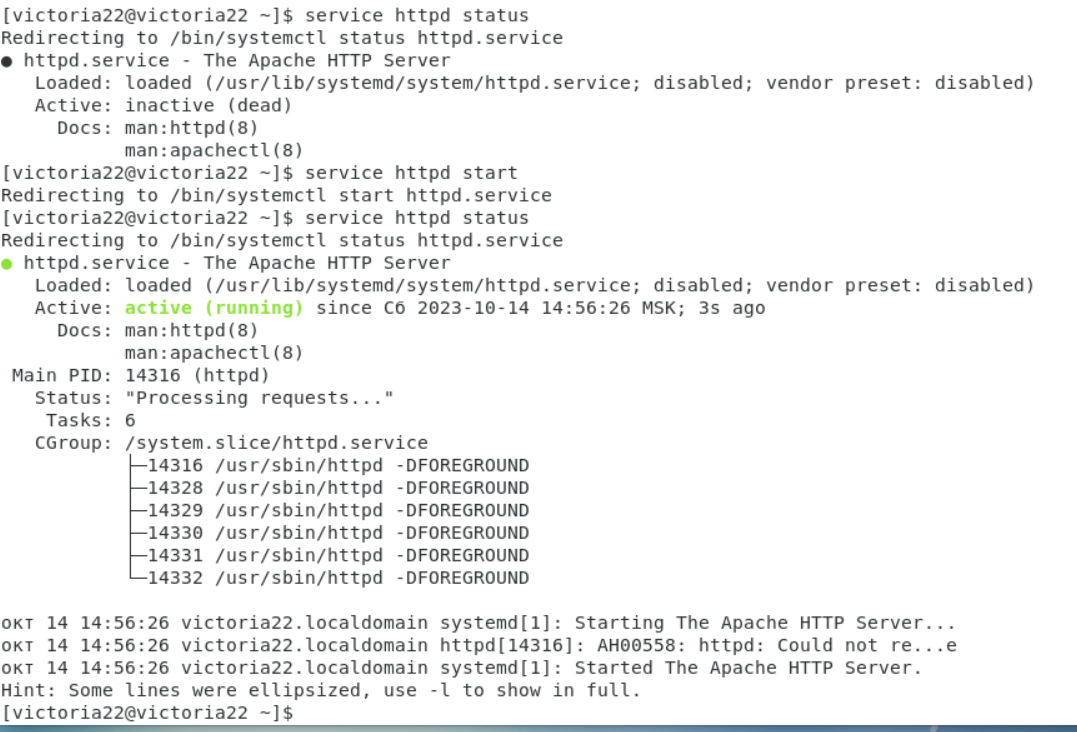


Figure 2: Обращение к веб-серверу

1. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности (рис. [3](#fig:003)).



Figure 3: Контекст безопасности веб-сервера Apache

1. Посмотрела текущее состояние переключателей SELinux для Apache (рис. [4](#fig:004)).

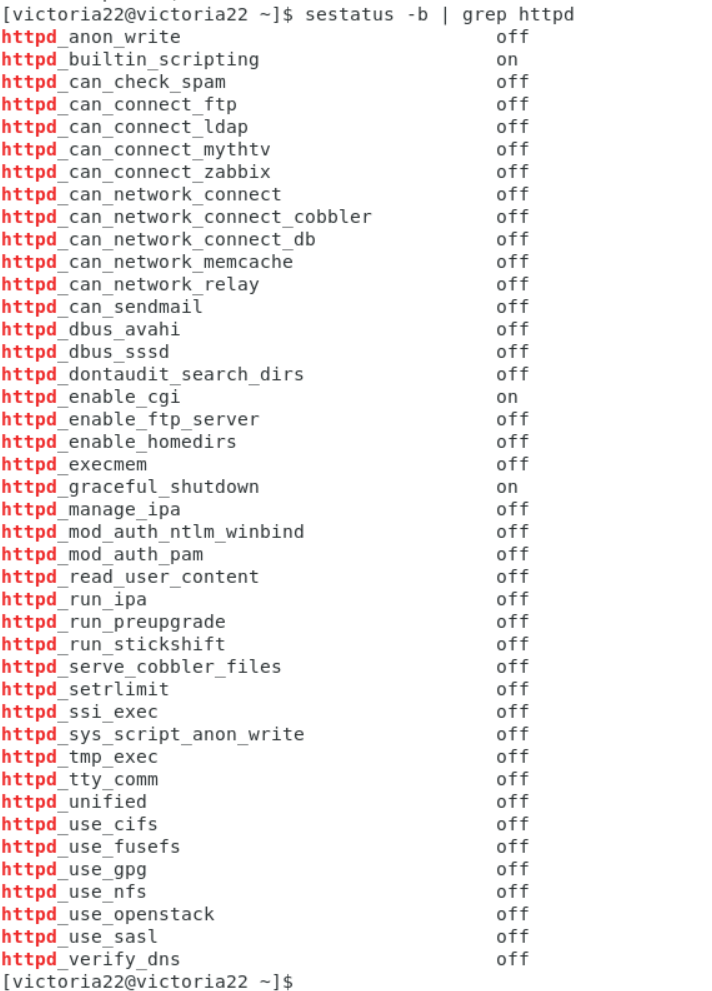


Figure 4: Текущее состояние переключателей SELinux для Apache

1. Посмотрела статистику по политике с помощью команды seinfo (рис. [5](#fig:005)).

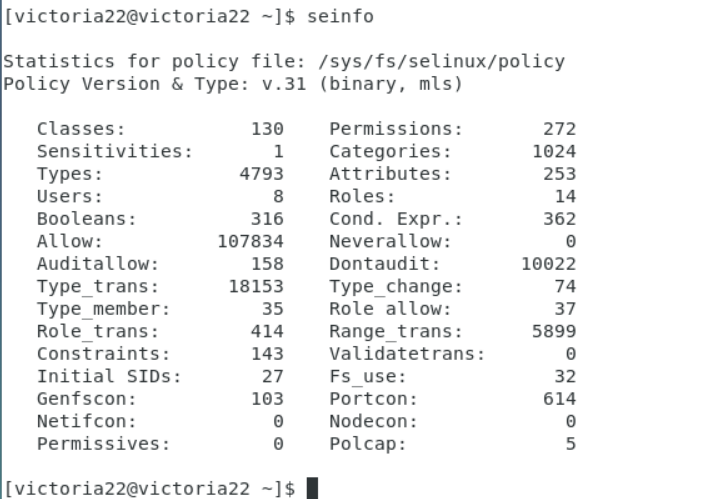


Figure 5: Статистика по политике

1. Определила тип файлов и поддиректорий, находящихся в директории /var/www (рис. [6](#fig:006)).

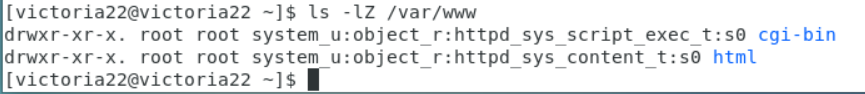


Figure 6: Тип файлов и поддиректорий, находящихся в директории /var/www

1. Определила тип файлов, находящихся в директории /var/www/html.
2. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html.
3. Создала от имени суперпользователя html-файл /var/www/html/test.html (рис. [7](#fig:007))(рис. [8](#fig:008))

Figure 7: Создание файла /var/www/html/test.html

Figure 7: Создание файла /var/www/html/test.html

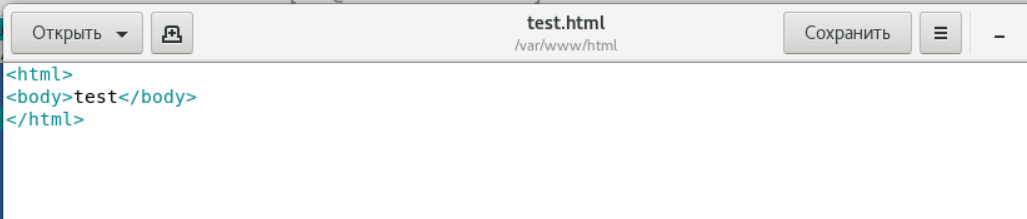
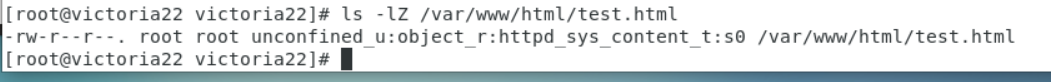


Figure 8: Создание файла /var/www/html/test.html

1. Проверила контекст созданного файла (рис. ??)  По умолчанию присваивается контекст unconfined\_u:object\_r:httpd\_sys\_content\_t:s0
2. Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедилась, что файл был успешно отображён (рис. [9](#fig:010)).

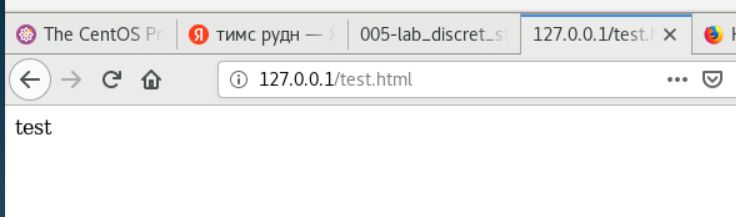


Figure 9: Файл test.html в браузере

1. Изучила справку man httpd\_selinux и выяснила, какие контексты файлов определены для httpd. Сопоставим их с типом файла test.html.
2. Изменила контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t (рис. [10](#fig:011)).

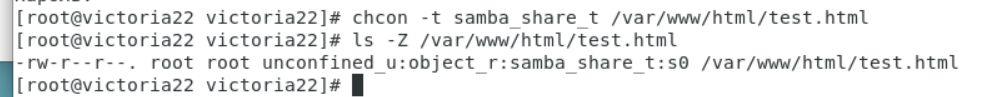
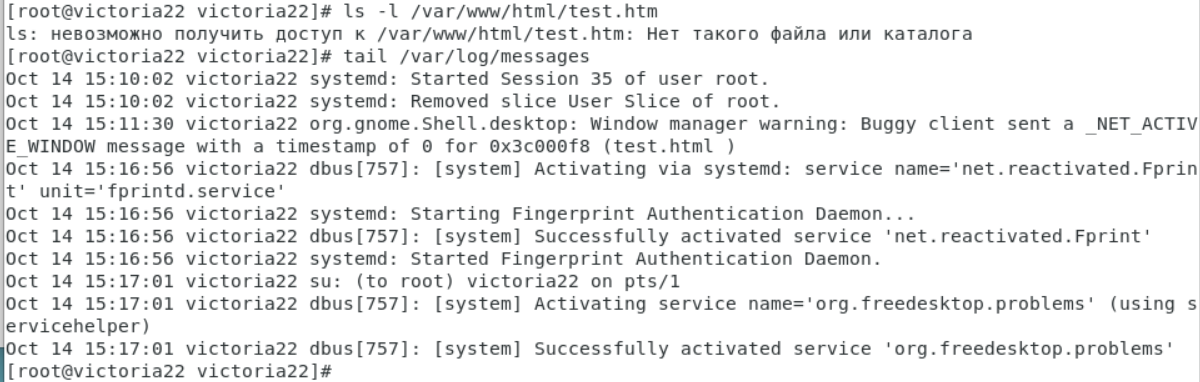


Figure 10: Изменение контекста

1. Попробовала ещё раз получить доступ к файлу через веб-сервер. В ответ получила запись Forbidden. You don’t have permission to access /test.html on this server.
2. Просмотрела log-файлы веб-сервера Apache и системный лог-файл (рис. ??).

 Мне не удалось получить доступ к файлу из-за измененного контекста.

1. Выполнила перезапуск веб-сервера. Сбоя не произошло.
2. Проанализировала лог-файлы.
3. Выполнила команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверила список портов командой semanage port -l | grep http\_port\_t (рис. [11](#fig:013)).

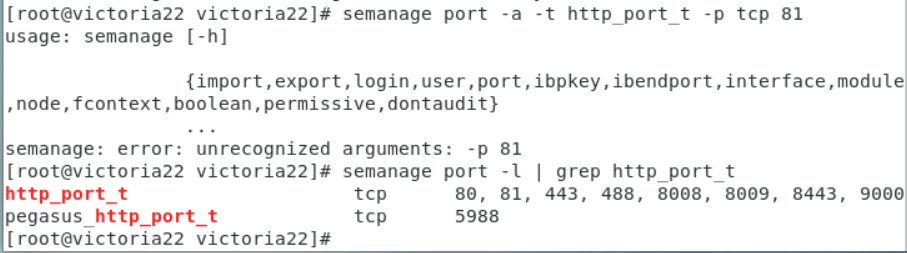


Figure 11: Попытка добавления порта 81 в список и вывод списка допустимых портов

1. Попробовала удалить привязку http\_port\_t к 81. Удаление невозможно. Удалила файл /var/www/html/test.html (рис. [12](#fig:014)).

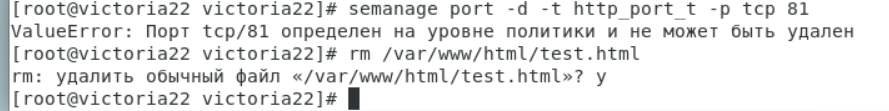


Figure 12: Попытка удаления привязки к порту 81. Удаление файла /var/www/html/test.html

# 3 Выводы

В рамках данной лабораторной работы были развиты навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux1. Проверена работа SELinx на практике совместно с веб-сервером Apache.

# 4 Список литературы

[1][Методический материал] [https://esystem.rudn.ru/pluginfile.php/2090279/mod\_resource/content/2/005-lab\_discret\_sticky.pdf] [2][Методический материал] [https://esystem.rudn.ru/pluginfile.php/2090282/mod\_resource/content/2/006-lab\_selinux.pdf]