Отчет по лабораторной работе №6

по дисциплине: Информационная безопасность

Го Чаопэн

Содержание

# Цели работы

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

# Задание

1. Настроить и запустить сервер Apache.
2. Исследовать влияние параметров сервера на его работу.

# Теоретическое введение

* Операционная система — это комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем [1].
* Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы. [2].

# Выполнение лабораторной работы

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

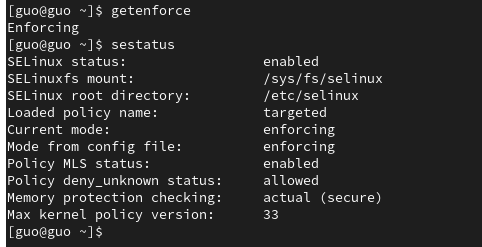


Figure 1: Конфигурация SELinux

1. Обратимся с помощью браузера к веб-серверу, запущенному на нашем компьютере, и убедимся, что последний работает ([2](#fig:002)).

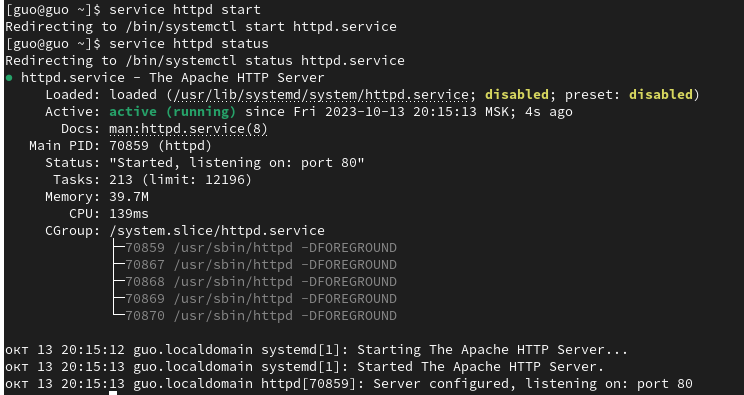


Figure 2: Обращение к веб-серверу

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

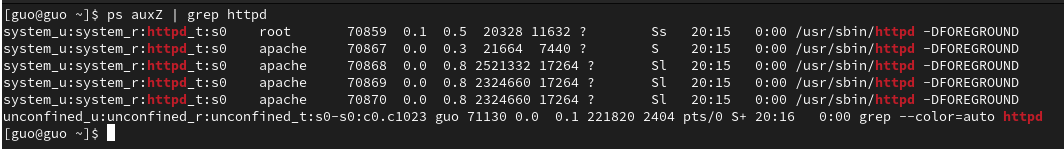


Figure 3: Контекст безопасности веб-сервера Apache

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

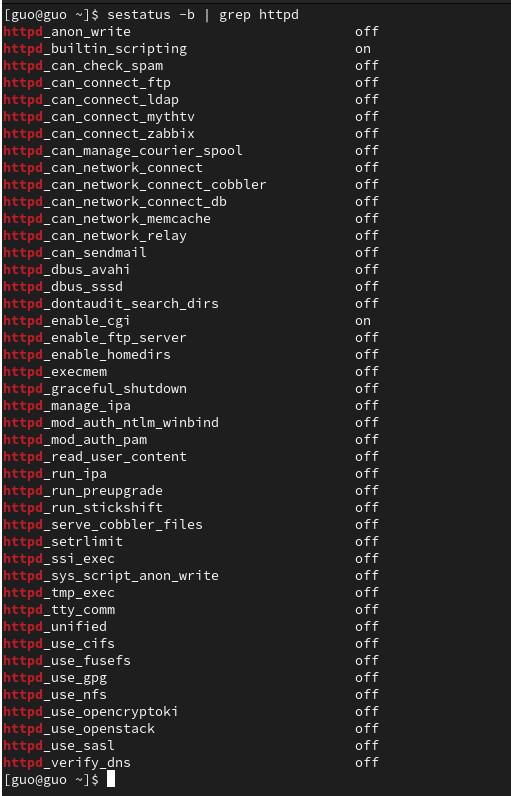


Figure 4: Текущее состояние переключателей SELinux для Apache

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

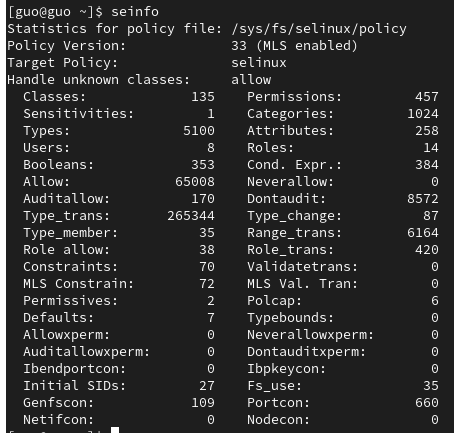


Figure 5: Статистика по политике

1. Определим тип файлов и поддиректорий, находящихся в директориях /var/www и /var/www/html. Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html([6](#fig:006)).

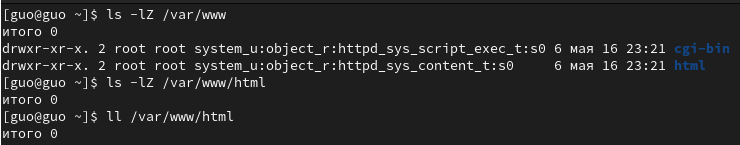


Figure 6: Тип файлов и поддиректорий, находящихся в директории /var/www

1. Создадим от имени суперпользователя html-файл /var/www/html/test.html. Проверим контекст созданного нами файла ([7](#fig:007)).

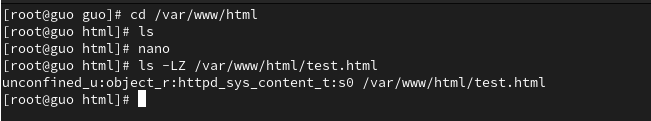


Figure 7: Создание файла /var/www/html/test.html

Заполним его следующим содержимым:

<html>  
 <body>test</body>  
</html>

Как видим по умолчанию присваивается контекст *unconfined\_u:object\_r:httpd\_sys\_content\_t:s0*

1. Обратимся к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедимся, что файл был успешно отображён ([8](#fig:008)).

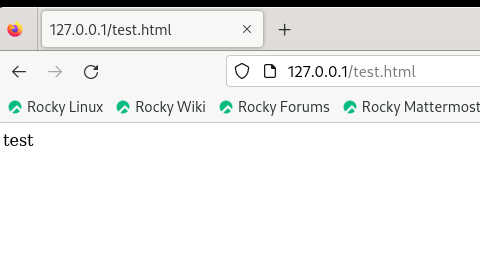


Figure 8: Файл test.html в браузере

1. Изучим справку man httpd\_selinux и выясним, какие контексты файлов определены для httpd. Сопоставим их с типом файла test.html ([9](#fig:009)).

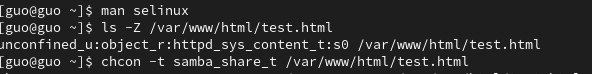


Figure 9: Вызов справки

1. Изменим контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t ([10](#fig:010)).

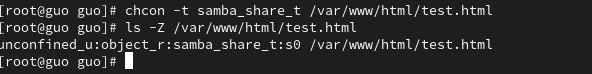


Figure 10: Изменение контекста

1. Попробуем ещё раз получить доступ к файлу через веб-сервер ([11](#fig:011)).

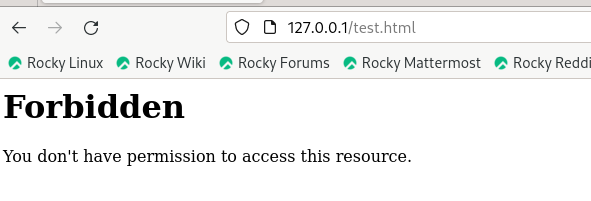


Figure 11: Файл test.html в браузере после изменения контекста

1. Просмотрим log-файлы веб-сервера Apache и системный лог-файл ([12](#fig:012)).

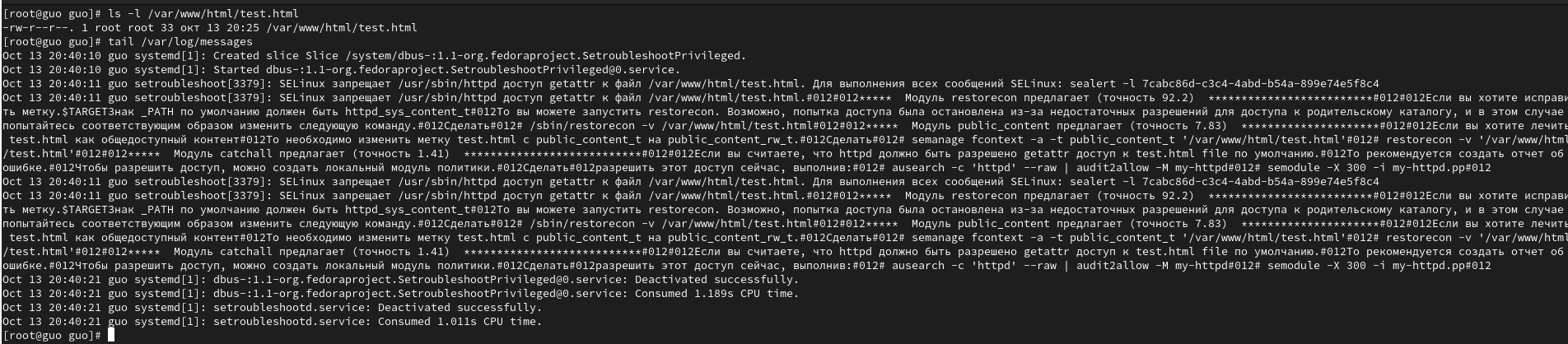


Figure 12: Содержимое логов

Как видим, нам не удалось получить доступ к файлу как раз из-за измененного контекста.

1. Попробуем запустить веб-сервер Apache на прослушивание ТСР-порта 81. Выполним перезапуск веб-сервера. Сбоя не произошло ([13](#fig:013)).

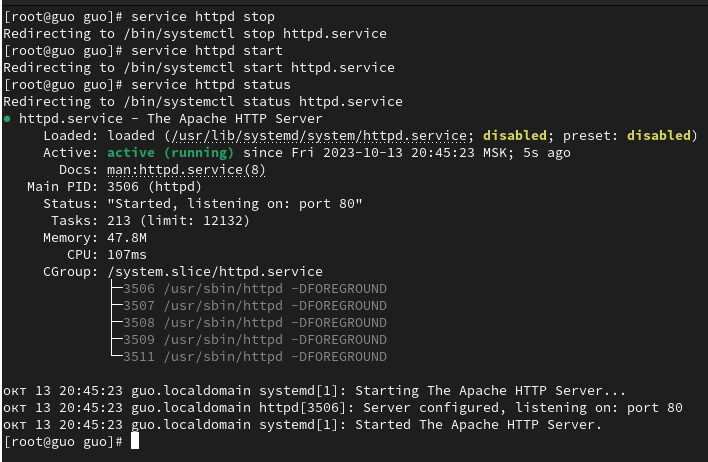


Figure 13: Изменение содержимого файла /etc/httpd/httpd.conf

1. Проанализируем лог-файлы ([14](#fig:014)).

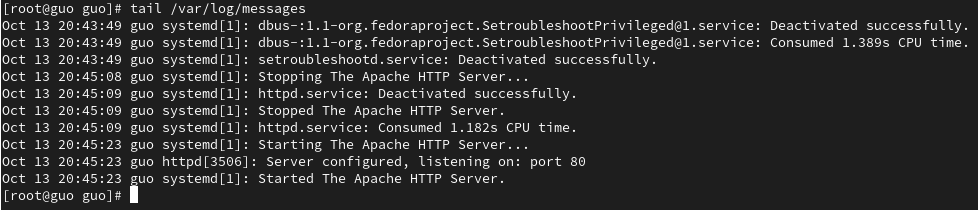


Figure 14: Лог-файл tail -nl /var/log/messages

1. Выполним команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверим список портов командой semanage port -l | grep http\_port\_t Убедимся, что порт 81 есть в списке. ([15](#fig:015)).

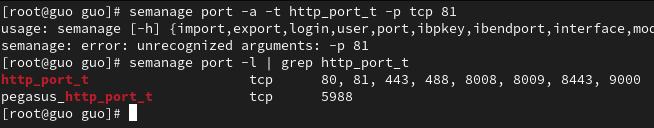


Figure 15: Попытка добавления порта 81 в список и вывод списка допустимых портов

1. Попробуем запустить веб-сервер Apache ещё раз. Вернем контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html. Попробуем получить доступ к файлу через веб-сервер ([16](#fig:016)).

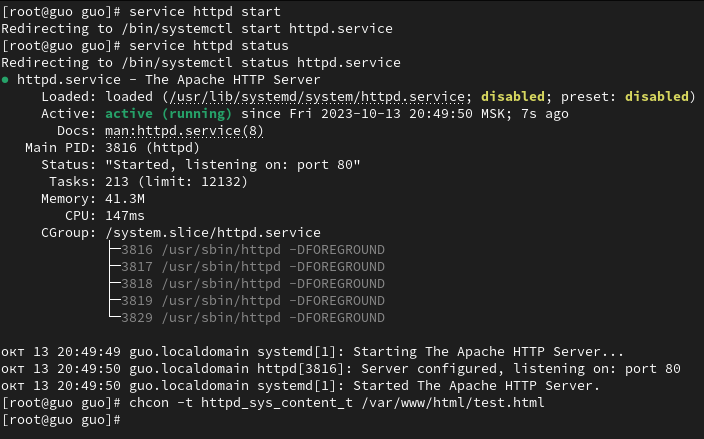


Figure 16: Повторный запуск веб-сервера

1. Исправим обратно конфигурационный файл apache, вернув Listen 80. Попробуем удалить привязку http\_port\_t к 81. Удалим файл /var/www/html/test.html ([17](#fig:017)).

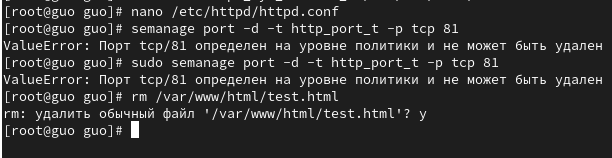


Figure 17: Попытка удаления привязки к порту 81

# 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.

# Список литературы

1. Операционные системы [Электронный ресурс]. URL: <https://softline.tm/solutions/programmnoe-obespechenie/operating-system>.

2. Права доступа [Электронный ресурс]. URL: <https://w.wiki/7UBB>.