Лабораторная работа № 6

Дисциплина: Информационная безопасность

Сулицкий Богдан Романович

Содержание

# 1 Цель работы

Целью данной лабораторной работы является развитие навыков администрирования ОС Linux и получение первого практического знакомства с технологией SELinux

# 2 Выполнение лабораторной работы

1. Я вошёл в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted. Далее я убедился, что веб-сервер работае(??).

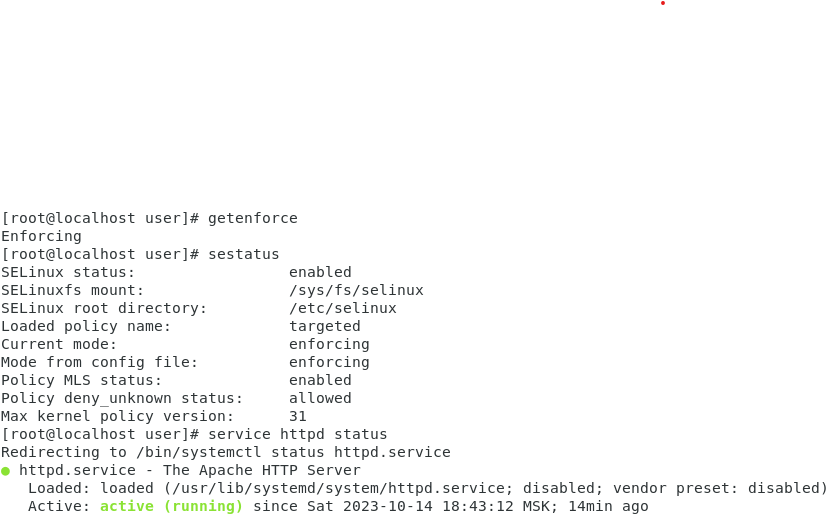


Рис. 1: Getenforce, sestatus и service status

1. Я нашёл веб-сервер Apache в списке процессов и посмотрел текущее состояние переключателей SELinux для Apache(??).

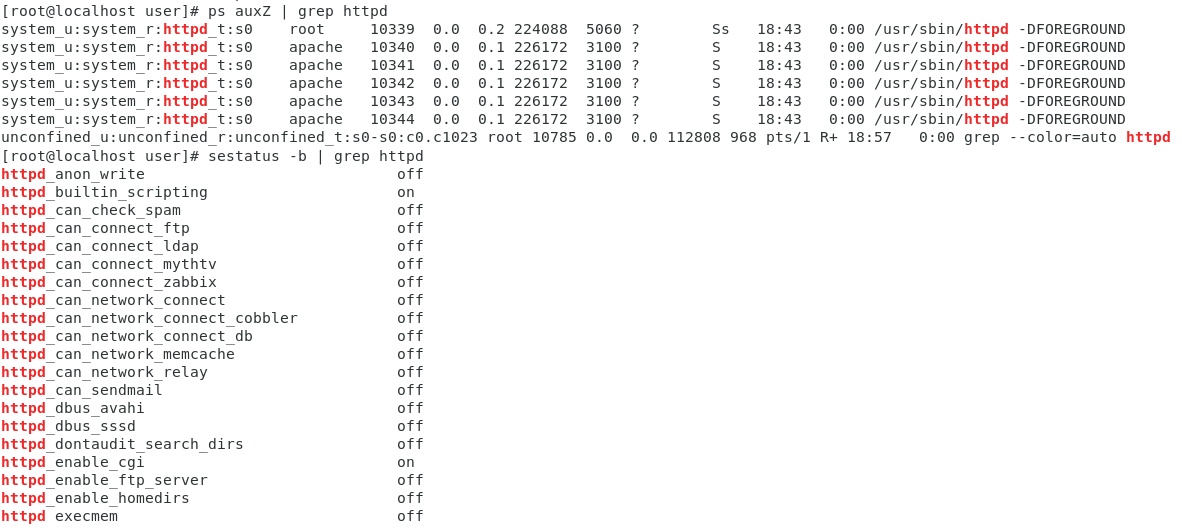


Рис. 2: Apache в списке процессов и состояния переключателей

1. Я посмотрел статистику по политике с помощью команды seinfol: 4793 типа, 8 пользователей и 14 ролей(??).

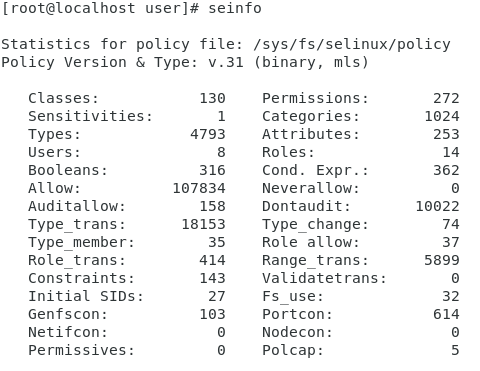


Рис. 3: Статистика по политике

1. Я определил тип файлов и поддиректорий, находящихся в директории /var/www. Далее я определил тип файлов в директории /var/www/html, и круг пользователей, которым разрешено создание файлов(??).



Рис. 4: Проверка данных /var/www/ и /var/www/html

1. Я создал от имени суперпользователя html-файл(??).

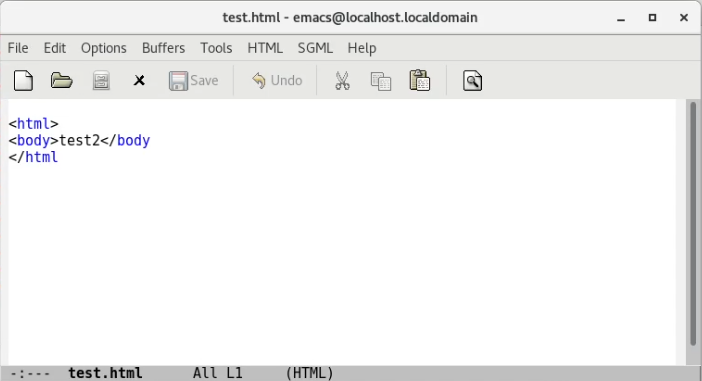


Рис. 5: Содержимое файла test.html

1. Я проверил контекст созданного мною файла(??).

Проверка контектса файла

Рис. 6: Проверка контектса файла

1. Я обратился к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html.(??).

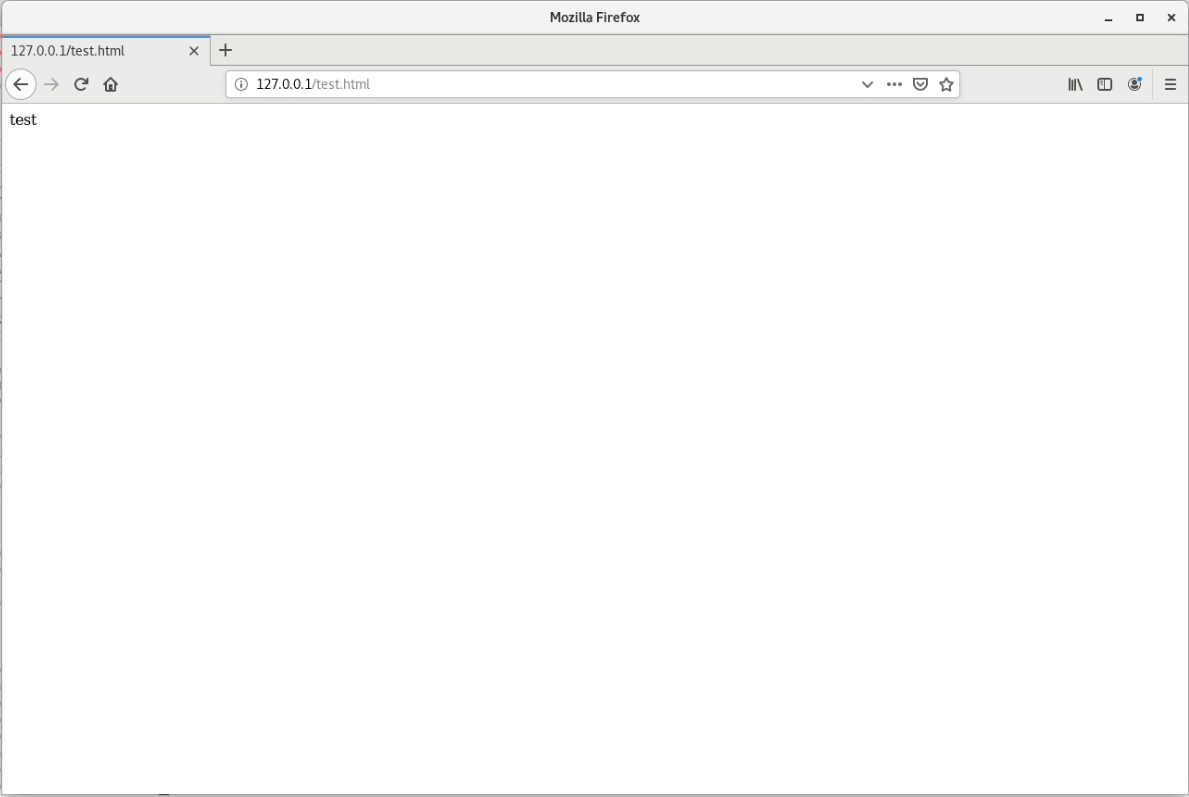


Рис. 7: Отображение файла в браузере 1

Файл был успешно отображён.

1. Я попробовал изучить справку man httpd\_selinux, однако получил ошибку. Далее я изменил контекст файла test.html на samba\_share\_t(??).

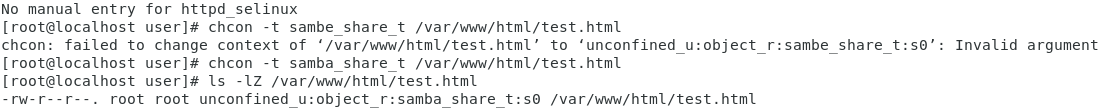


Рис. 8: Изменение контекста файла test.html 1

1. Я обратился к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получил ошибку Forbidden(??).

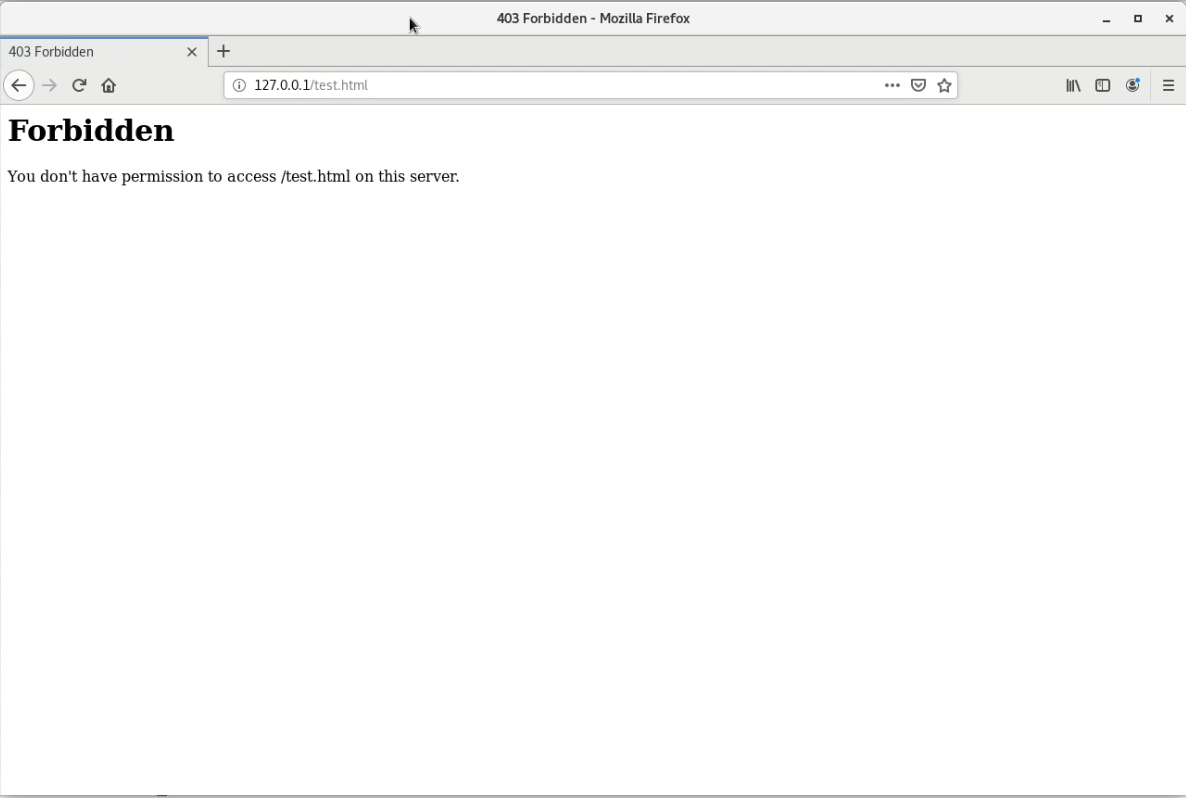


Рис. 9: Отображение файла в браузере 2

1. Я изучил права доступа на файл test.html, просмотрел log-файлы и файл аудита(??).



Рис. 10: Просмотр информации о файле test.html и вывод log-файлов

Audit.log и log-файлы содержат в себе данные об отказе в доступе.

1. Я попробовал запустить веб-сервер Apache на прослушивание ТСР-порта 81(??).

Изменения порта 1

Рис. 11: Изменения порта 1

И попробовал перезапустить веб-сервер(??).

Перезапуск веб-сервера 1

Рис. 12: Перезапуск веб-сервера 1

Сервер перезапустился. Никаких сбоев не было, так 81 порт по умолчанию используется в пуле.

1. Я проанализировал лог-файлы(??).

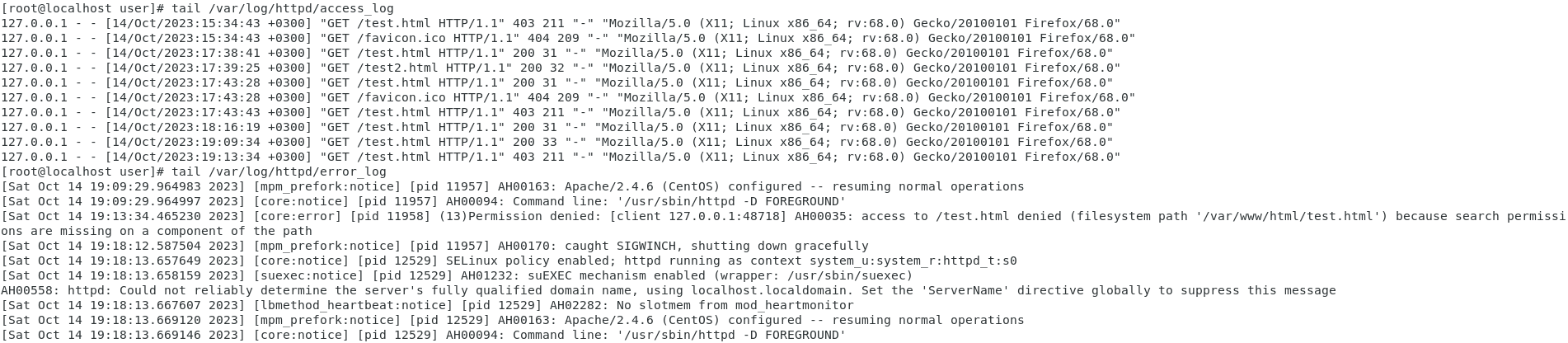


Рис. 13: Access\_log и error\_log

Никаких новый записей не появилось.

1. Я выполнил команду привязки порта и получил ошибку, так как порт уже определен. Далее я проверил список портов(??).

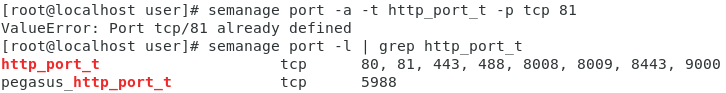


Рис. 14: Привязка порта и проверка списка портов

1. Я попробовал перезапустить веб-сервер. Он успешно перезапустился, как и в предыдущий раз(??).

Перезапуск веб-сервера 2

Рис. 15: Перезапуск веб-сервера 2

1. Я вернул контекст httpd\_sys\_cоntent\_\_t к файлу test.html(??).

Изменение контекста файла test.html 2

Рис. 16: Изменение контекста файла test.html 2

После этого я попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html (??).

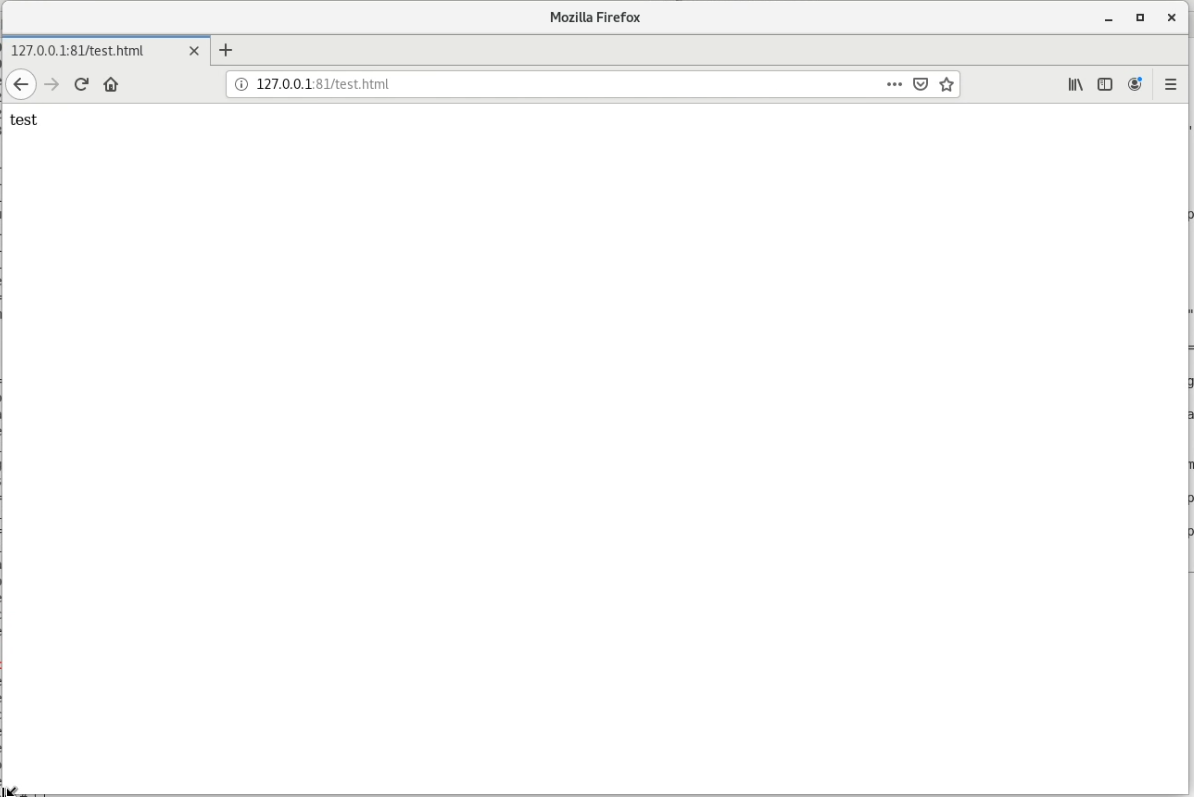


Рис. 17: Отображение файла в браузере 3

Файл был успешно отображён.

1. Я исправил обратно конфигурационный файл apache, вернув Listen 80(??).

Изменения порта 2

Рис. 18: Изменения порта 2

1. Я попробовал удалить привязку http\_port\_t к 81 порту, но поскольку данный порт определен политикой, я не смог исполнить эту команду. Далее я удалил файл test.html с помощью команды rm(??).

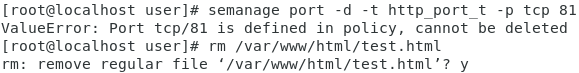


Рис. 19: Удаление привязки порта и удаление файла test.html

# 3 Вывод

В ходе проделанной лабораторной работы я развил свои навыки администрирования ОС Linux и получил первое практическое знакомствое с технологией SELinux

# Список литературы

[1] https://esystem.rudn.ru/pluginfile.php/2090282/mod\_resource/content/2/006-lab\_selinux.pdf