Лабораторная работа №6

Мандатное разграничение прав в Linux

Аскеров Александр Эдуардович

Содержание

[1 Цель работы 1](#__RefHeading___Toc370_3723719555)

[2 Выполнение лабораторной работы 1](#__RefHeading___Toc372_3723719555)

[3 Выводы 9](#__RefHeading___Toc374_3723719555)

[Список литературы 9](#__RefHeading___Toc376_3723719555)

# 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 Выполнение лабораторной работы

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

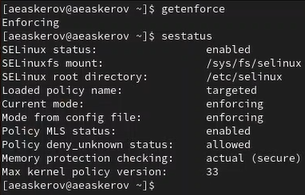


Рис. 1: Проверка SELinux

Обратимся с помощью браузера к веб-серверу, запущенному на компьютере, и убедимся, что последний работает.

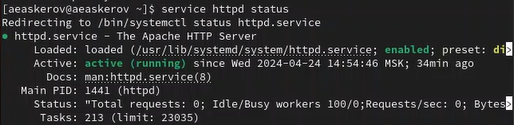


Рис. 2: Проверка работы веб-сервера

Найдём веб-сервер Apache в списке процессов, определим его контекст безопасности.

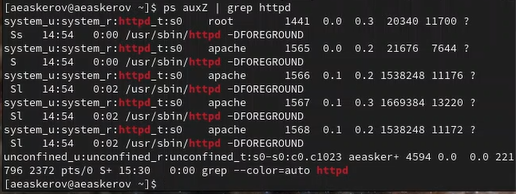


Рис. 3: Контекст безопасности веб-сервера

Посмотрим текущее состояние переключателей SELinux для Apache.

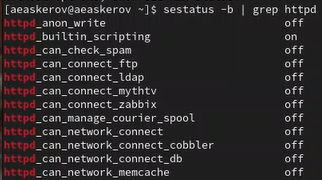


Рис. 4: Переключатели SELinux

Посмотрим статистику по политике с помощью команды seinfo, также определим множество пользователей, ролей, типов.

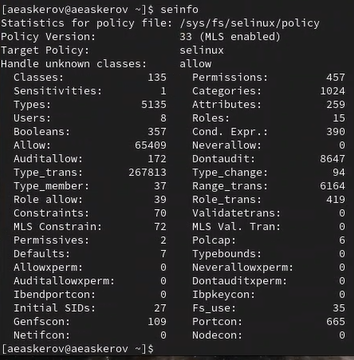


Рис. 5: Статистика по политике

Определим тип файлов и поддиректорий, находящихся в директории /var/www.

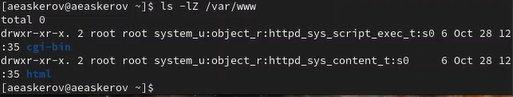


Рис. 6: Тип файлов и поддиректорий

Определим тип файлов, находящихся в директории /var/www/html.

Рис. 7: Тип файлов

Рис. 7: Тип файлов

Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html.

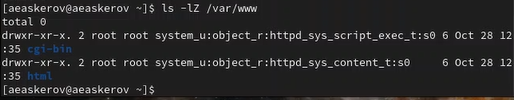


Рис. 8: Круг пользователей с разрешением

Создадим от имени суперпользователя html-файл /var/www/html/test.html следующего содержания.

Рис. 9: html-файл

Рис. 9: html-файл

Проверим контекст созданного файла. Запишем контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.

Рис. 10: Контекст файла

Рис. 10: Контекст файла

Обратимся к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html.

Изучим справку man httpd\_selinux.

Изменим контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba\_share\_t.

Рис. 11: Изменение контекста

Рис. 11: Изменение контекста

Рис. 12: Проверка контекста

Рис. 12: Проверка контекста

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

Проанализируем ситуацию. Просмотрим log-файлы веб-сервера Apache. Также просмотрим системный лог-файл.

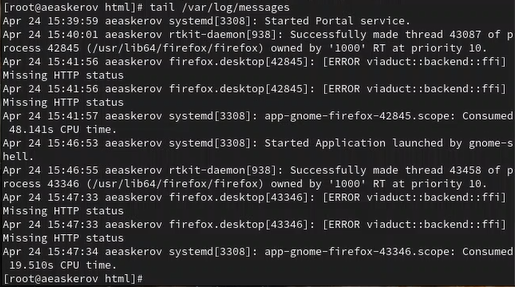


Рис. 13: Системный лог-файл

Посмотрим файл /var/log/audit/audit.log.

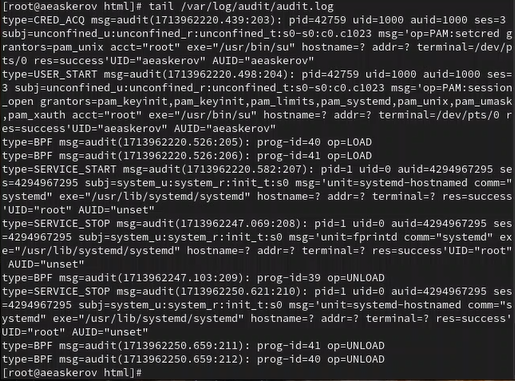


Рис. 14: Файл audit.log

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 найдём строчку Listen 80 и заменим её на Listen 81.

Рис. 15: Изменение порта

Рис. 15: Изменение порта

Выполним перезапуск веб-сервера Apache. Произошёл сбой из-за изменения порта.

Проанализируем лог-файлы.

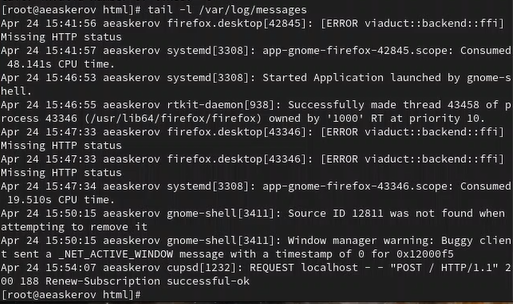


Рис. 16: Файл messages

Просмотрим файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выясним, в каких файлах появились записи.

Рис. 17: Файл access_log

Рис. 17: Файл access\_log

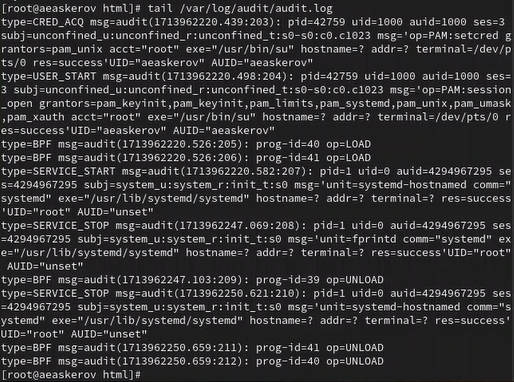


Рис. 18: Файл audit.log

Выполним следующую команду.

Рис. 19: Управление портами

Рис. 19: Управление портами

Рис. 20: Управление портами

Рис. 20: Управление портами

Порт 81 появился в списке.

Попробуем запустить веб-сервер Apache ещё раз. Теперь он запустился.

Вернём контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/test.html.

Рис. 21: Возврат контекста

Рис. 21: Возврат контекста

После этого попробуем получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html.

Мы видим содержимое файла – слово «test».

Исправим обратно конфигурационный файл apache, вернув Listen 80.

Рис. 22: Изменение порта

Рис. 22: Изменение порта

Удалим привязку http\_port\_t к 81-му порту.

Рис. 23: Удаление привязки

Рис. 23: Удаление привязки

Удалим файл /var/www/html/test.html.

Рис. 24: Удаление файла

Рис. 24: Удаление файла

# 3 Выводы

Развиты навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux.

Проверена работа SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. [Веб-сервер Apache](https://httpd.apache.org/)