Лабораторная работа 6

Мандатное разграничение прав в Linux

Лушин Артём Андреевич

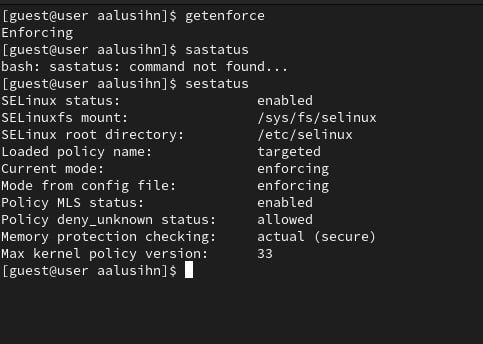
Содержание

# 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.

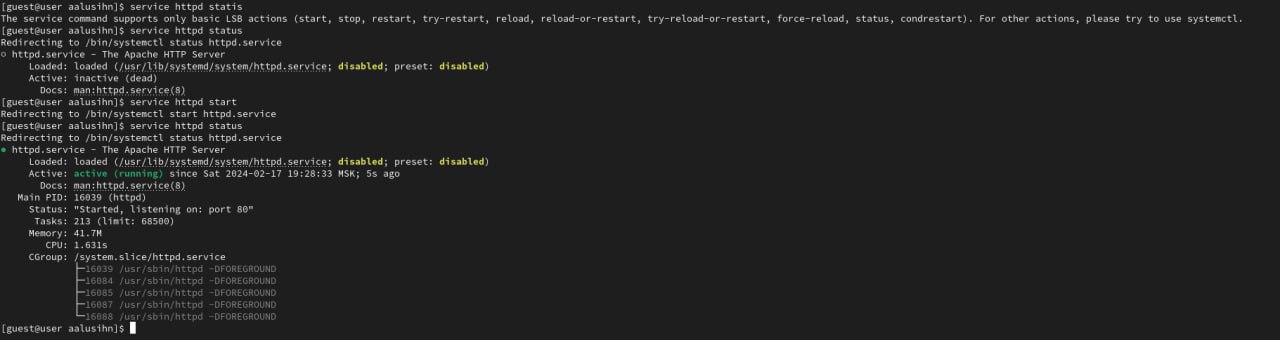
# 2 Выполнение лабораторной работы

1. Я проверил в каком режиме работает SELinux. Режим - Enforcing, а политика - targeted.



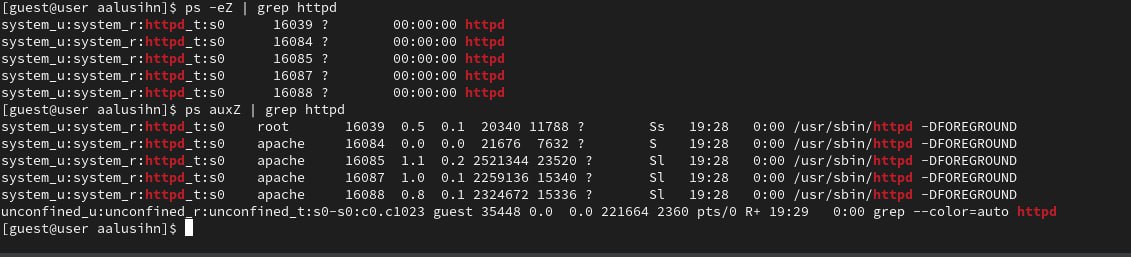
Проверка режима и политики

1. Проверил статус браузера к веб-серверу, который запущен на компьютере. Статус - active.



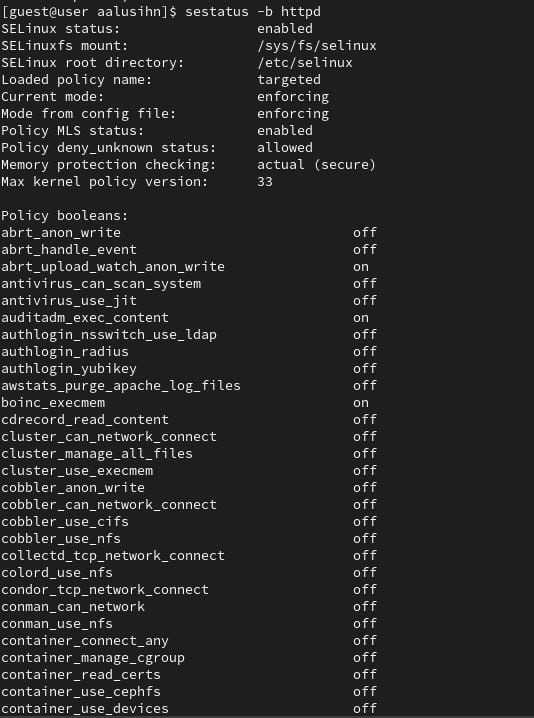
Проверка статуса

1. Я определил контекст безопасности веб-сервера Apache. Контекст - httpd\_t.



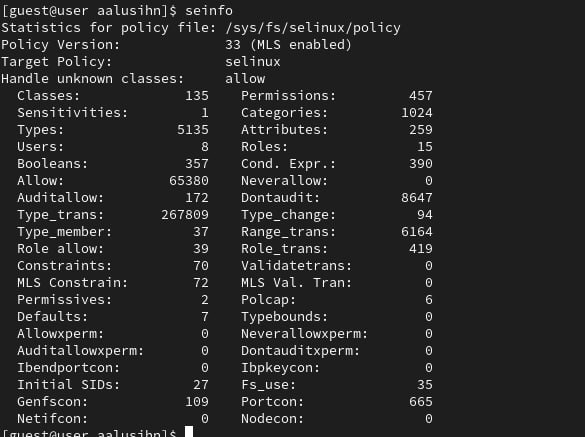
Определение контекста безопасности

1. Посмотрел текущее состояние переключателей SELinux для Apache. Большая часть переключателей выключены.



Проверка переключателей

1. Посмотрел статистику по политике. Пользователей - 8, ролей - 15, а типов - 5135.



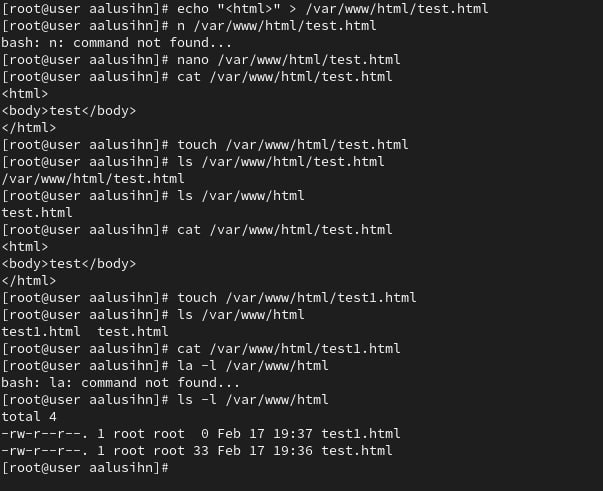
Статистика политики

1. Определил тип файлов, которые находятся в директории “/var/www/html”. Все файлы созданы и относятся к пользователю root. Владельцем так же является пользователь root.



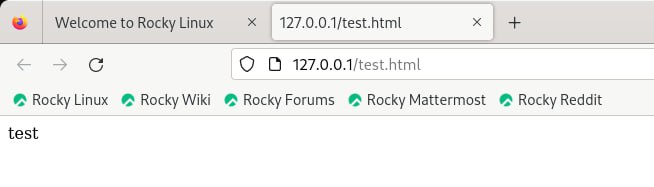
Тип файлов html

1. От имени суперпользователя создал файл “test.html” в директории “/var/www/html”. Вписал туда необходимый текст, чтобы потом проверить его на сайте. А контекст для новых файлов - httpd\_sys\_content\_t.



Создание файла

1. Я ввёл в браузере ссылку “http://127.0.0.1/test.html”. Файл успешно отобразился и на сайте показали такой же текст, как и в файле.



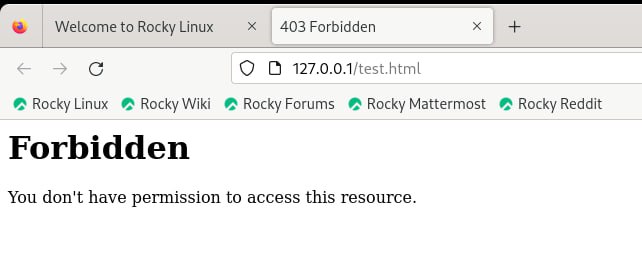
Отображение на сайте

1. Я изучил справку “man httpd\_selinux”. Для httpd определены следующие контексты: httpd\_sys\_conten\_t, httpd\_sys\_script\_exec\_t, httpd\_sys\_script\_ro\_t, httpd\_sys\_script\_rw\_t, httpd\_sys\_script\_ra\_t, httpd\_unconfined\_script\_exec\_t. Я изменил контекст моего файла на “samba\_share\_t и провели, чтобы контекст установился.



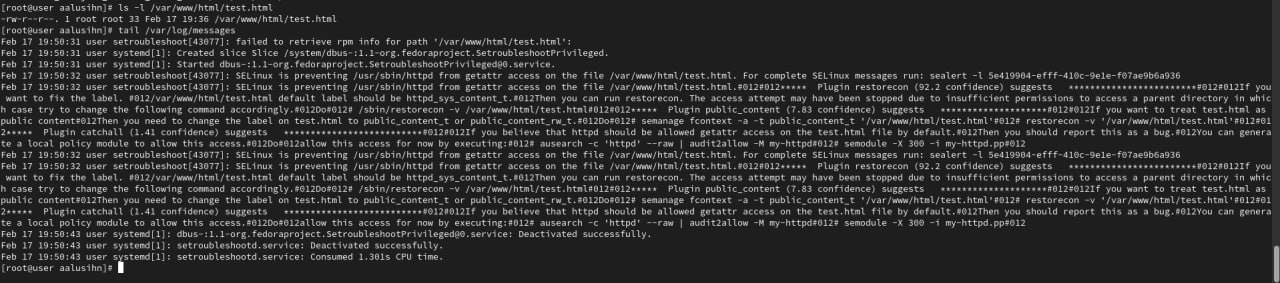
Смена контекста

1. Я попытался подключиться к файлу на сайте, но выдало ошибку. Связано это с тем, что httpd не имеет доступа к тому контексту, который я установил.



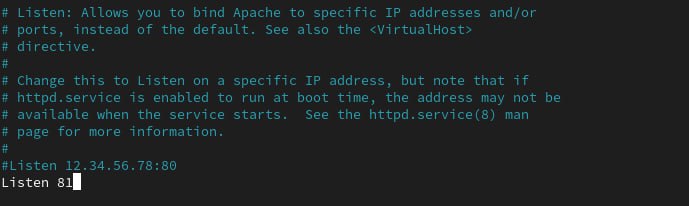
Проверка нового контекста

1. Я убедился, что есть права доступа на чтение, но ошибка появляется из-за того, что сам httpd не может распознать контекст. Так же просмотрел системный лог-файл веб-сервера Apache и увидел, что он отображает ошибки.



Проверка лог-файла

1. В файле “/etc/httpd/conf/httpd.conf” изменил TCP-порт на 81, а не на 80, как рекомендована IANA.



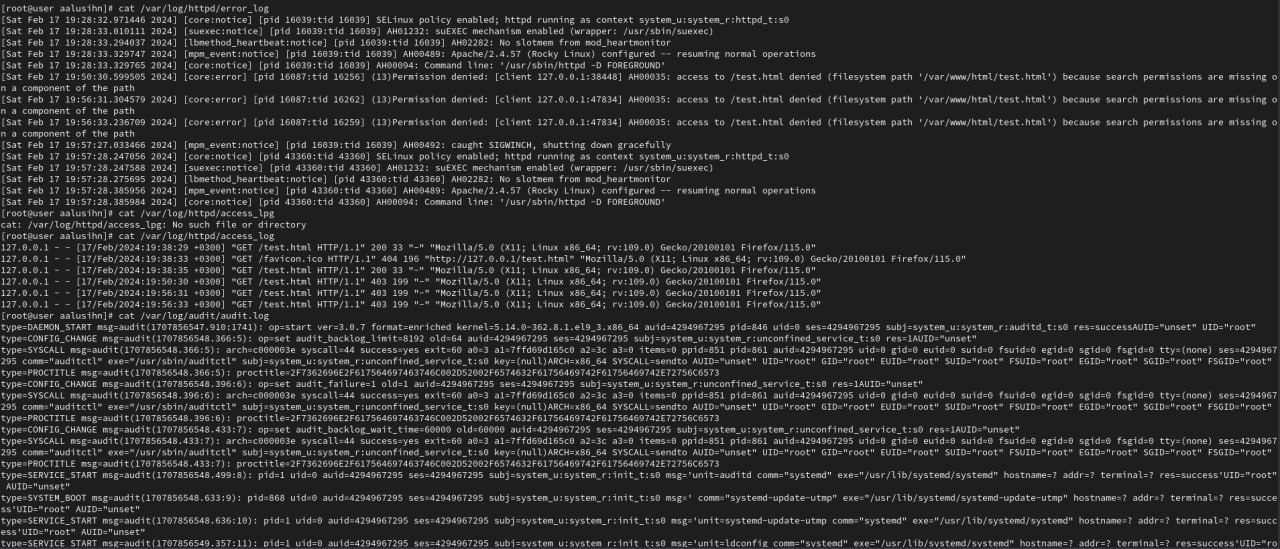
Изменение порта на 81

1. Я перезапустил сервер и проанализировал лог-файл.



Перезапуск сервера

1. Я просмотрел файлы “/var/log/http/error\_log”, “/var/log/http/access\_log” и “/var/log/audit/audit.log”. Изменения произошли в audit файле.



Проверка файлов

1. Я выполнил команду для смены портов и затем проверил список портов, чтобы убедиться, что появился 81 порт.

![Смена портов](data:application/octet-stream;base64,)

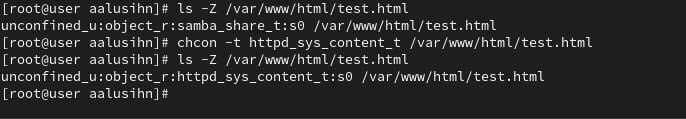
Смена портов

1. Я перезапустил веб-сервер и он запустился. Произошло это из-за того, что я добавил порт, которого до этого не было.



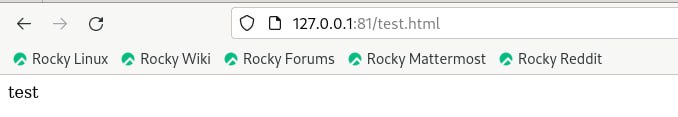
Перезапуск веб-сервера с добавленным портом

1. Я вернул изначальный контекст файлу “text.html” и убедился в этом.



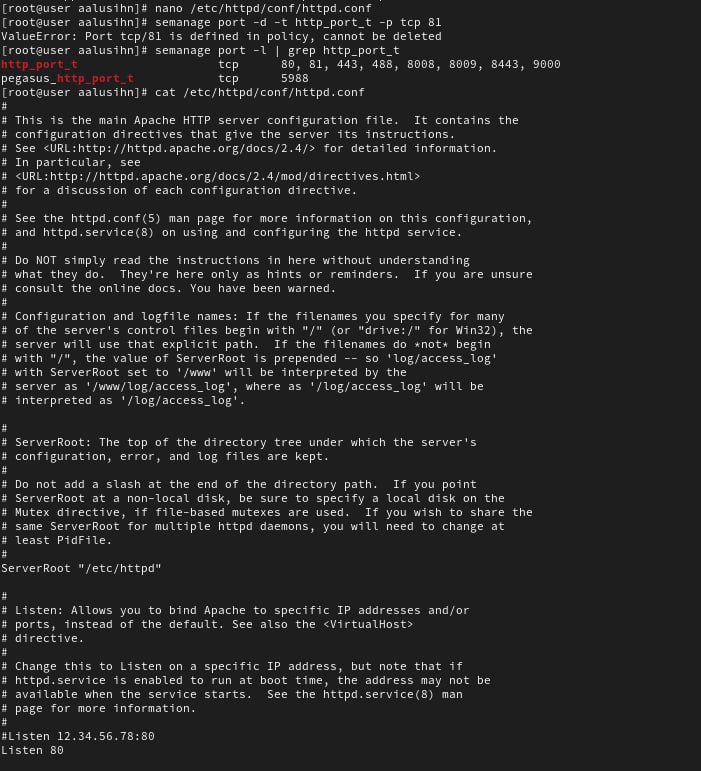
Возвращение контекста

1. Попробовал зайти на веб-сервер, чтобы убедиться в том, что файл читается. Веб-сервер подключился и вывел текст “test”, как и в самом файле. Даже не смотря на то, что я поменял порт, веб-сервер запустился.



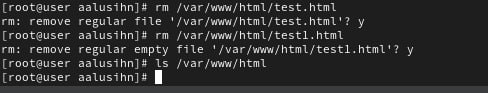
Проверка веб-сервера с новым портом

1. Я исправил в конфигурационном файле 80 порт. Попытался вообще удалить привязку 81 порта, но этого нельзя сделать, так как не разрешает политика. Но тем не менее, теперь в конфигурационном файле стоит 80 порт и в списке портов он есть.



Возвращение старого порта

1. Чтобы в дальнейшем мне не мешались тестовые файлы, я удалил все файлы, с которым работал в директории “var/www/html”.



Удаление файлов

# 3 Выводы

Я развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.