Лабораторная работа №6

Мандатное разграничение прав в Linux

Серенко Д.С. группа НФИ-01-19

Содержание

# Цель работы

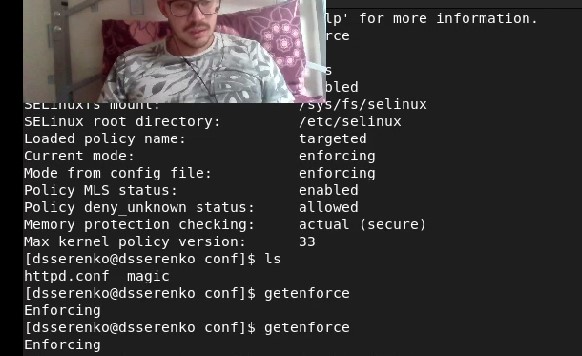
Целью данной лабораторной работы является развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Подготовка лабораторного стенда и методические рекомендации

1. Установили веб-сервер Apache.
2. В конфигурационном файле /etc/httpd/httpd.conf задали параметр ServerName.
3. Отключаем пакетный фильтр.

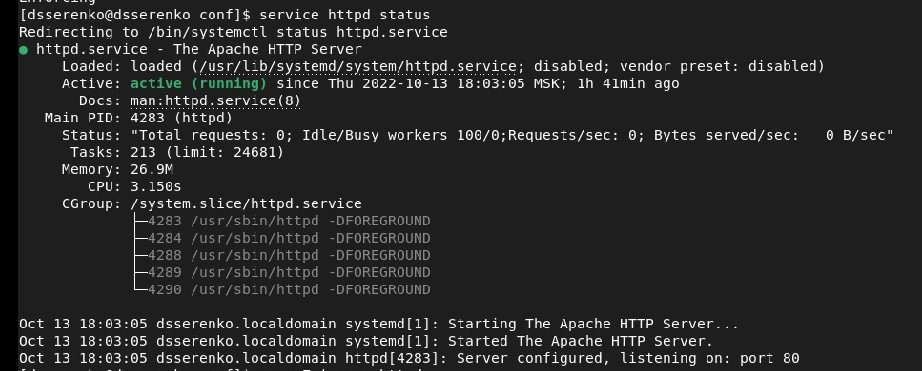
# Выполнение лабораторной работы

1. Входим в систему с полученными учётными данными. Проверили, что SELinux работает в режиме enforcing политики targeted с помощью команд **getenforce** и **sestatus**. (@fig:004)



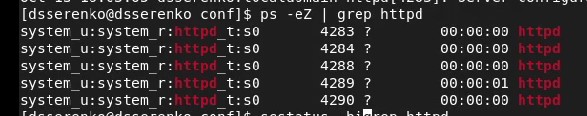
Выполнение команд getenforce и sestatus

1. Запустили веб-сервер и обратились к нему с помощью команды (@fig:005): service httpd status



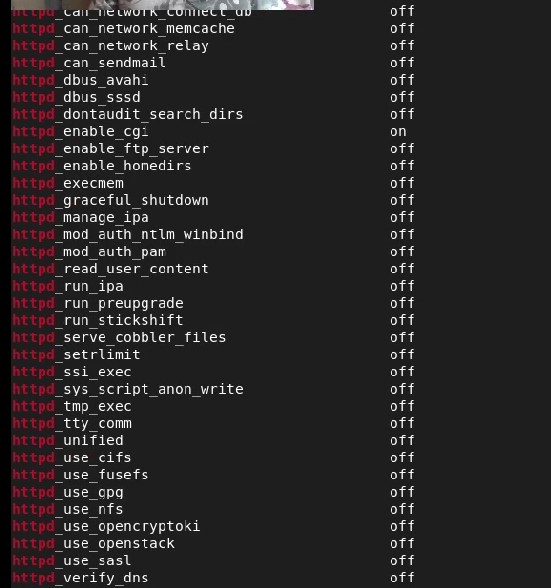
Выполнение команды service httpd status

1. Нашли веб-сервер Apache в списке процессов. Контекст безопасности - unconfined\_u:unconfined\_r:unconfined\_t. (@fig:006)



Выполнение команды ps auxZ | grep httpd

1. Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды **sestatus -b | grep httpd**. (@fig:007)



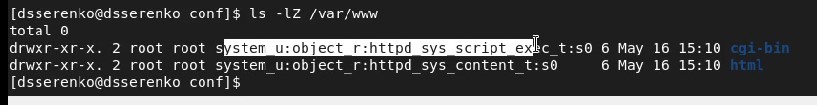
Выполнение команды sestatus -b | grep httpd

1. Посмотрели статистику по политике с помощью команды **seinfo**. Определили, что множество пользователей = 8; ролей = 14; типов = 5002. (@fig:008)



Статистика по политике

1. Определили тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды **ls -lZ /var/www**. (@fig:009)



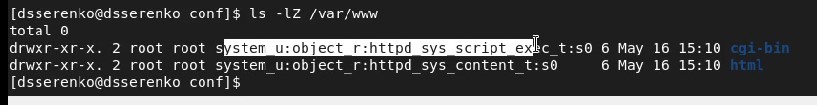
Выполнение команды ls -lZ /var/www

1. Необходимо было определить тип файлов, находящихся в директории /var/www/html, с помощью команды **ls -lZ /var/www/html**. Но в данной директории файлов не обнаружилось. (@fig:010)

Выполнение команды ls -lZ /var/www/html

Выполнение команды ls -lZ /var/www/html

1. Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html - только uesr. (@fig:011)



Выполнение команды ls -lZ /var/www

1. Создали от имени суперпользователя html-файл /var/www/html/test.html следующего содержания: (@fig:012)



Содержимое файла test.html

1. Проверили контекст созданного файла - httpd\_sys\_content\_t. (@fig:013)

Контекст файла test.html

Контекст файла test.html

1. Обратитились к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html и убедились, что файл был успешно отображён. (@fig:014)



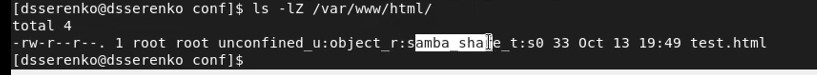
Обращение к файлу test.html через веб-сервер

1. Изучили справку man httpd\_selinux. Тип файла test.html - контекст созданного файла - httpd\_sys\_content\_t. (@fig:015)

Контекст файла test.html

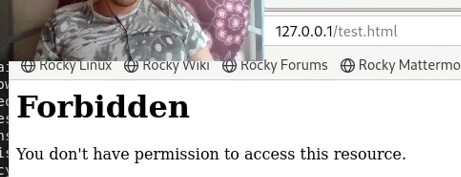
Контекст файла test.html

1. Изменили контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t: chcon -t samba\_share\_t /var/www/html/test.html ls -Z /var/www/html/test.html И проверили, что контекст поменялся. (@fig:016)



Изменение контекста файла /var/www/html/test.html

1. Пробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. В результате получили ошибку. (@fig:017)



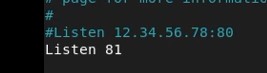
Обращение к файлу test.html через веб-сервер после изменения контекста

1. Проанализируем ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? ls -l /var/www/html/test.html Просмотрим log-файлы веб-сервера Apache и системный лог-файл: tail /var/log/messages В системе оказались запущенны процессы **setroubleshootd** и **audtd**. (@fig:018)



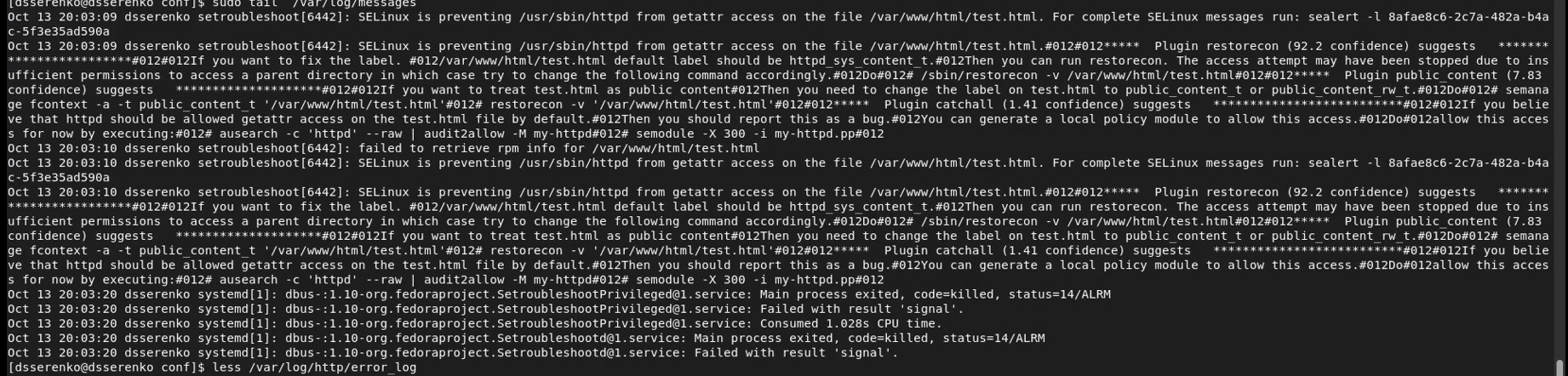
Вывод команд ls -l /var/www/html/test.html и tail /var/log/messages

1. Попробуем запустить веб-сервер Apache на прослушивание ТСР-порта 81. Для этого в файле /etc/httpd/httpd.conf находим строчку Listen 80 и заменяем её на Listen 81. (@fig:019)



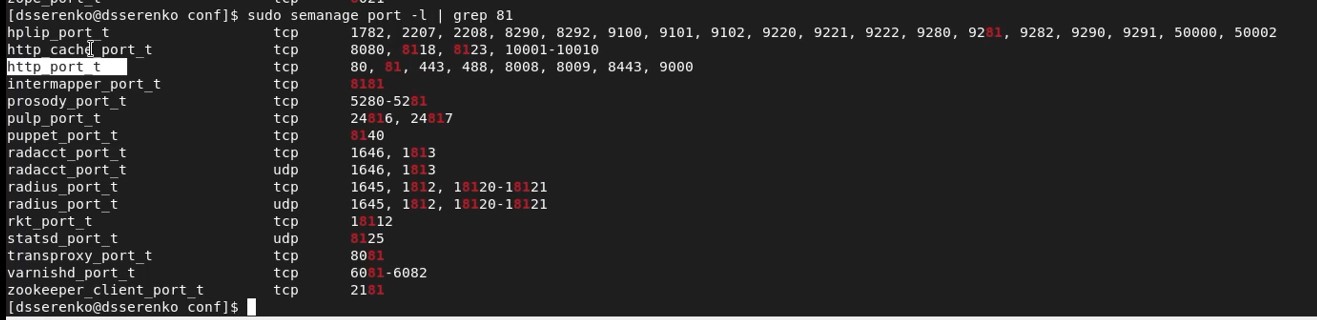
Запуск веб-сервера Apache на прослушивание ТСР-порта 81

1. Выполним перезапуск веб-сервера Apache. Произошёл сбой? Нет.
2. Проанализируем лог-файлы: tail -nl /var/log/messages Просмотрим файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log. (@fig:020)



Перезапуск веб-сервера Apache

1. Выполним команду **semanage port -a -t http\_port\_t -р tcp 81**. Вылетает ValueError в связи с тем, что порт уже определен. После этого проверим список портов командой **semanage port -l | grep http\_port\_t** и убедились, что порт 81 появился в списке. (@fig:021)



Проверка установления 81 порта tcp

1. Попробуем запустить веб-сервер Apache ещё раз. (@fig:022)

Перезапуск веб-сервера Apache

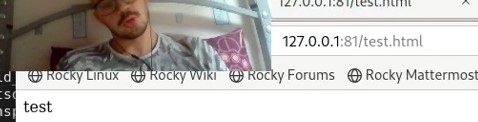
Перезапуск веб-сервера Apache

1. Вернули контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/test.html: **chcon -t httpd\_sys\_content\_t /var/www/html/test.html** (@fig:023)

Возвращение контекста httpd_sys_cоntent__t к файлу test.html

Возвращение контекста httpd\_sys\_cоntent\_\_t к файлу test.html

После этого пробуем получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. В результате увидели содержимое файла — слово «test». (@fig:024)



Обращение к файлу test.html через веб-сервер

1. Исправим обратно конфигурационный файл apache, вернув Listen 80. (@fig:025)

Исправление конфигурационного файла apache

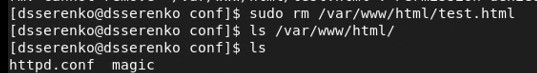
Исправление конфигурационного файла apache

1. Удалим привязку http\_port\_t к 81 порту: **semanage port -d -t http\_port\_t -p tcp 81** и проверим, что порт 81 удалён. Данная команда не была выполнена. (@fig:026)

Удаление привязки http_port_t к 81 порту

Удаление привязки http\_port\_t к 81 порту

1. Удалим файл /var/www/html/test.html: **rm /var/www/html/test.html**. (@fig:027)



Удаление файла test.html

# Вывод

В ходе выполнения лабораторной работы мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.

# Библиография

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Мандатное разграничение прав в Linux [Текст] / Кулябов Д. С., Королькова А. В., Геворкян М. Н. - Москва: - 5 с. [^1]: Мандатное разграничение прав в Linux.
2. Справочник 70 основных команд Linux: полное описание с примерами (https://eternalhost.net/blog/sozdanie-saytov/osnovnye-komandy-linux)