Лабораторная работа №6

Основы информационной безопасности

Колчева Юлия Вячеславовна

Содержание

# Цель работы

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

# Выполнение лабораторной работы

Вошла в систему под своей учетной записью и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд “getenforce” и “sestatus”(рис. 1)

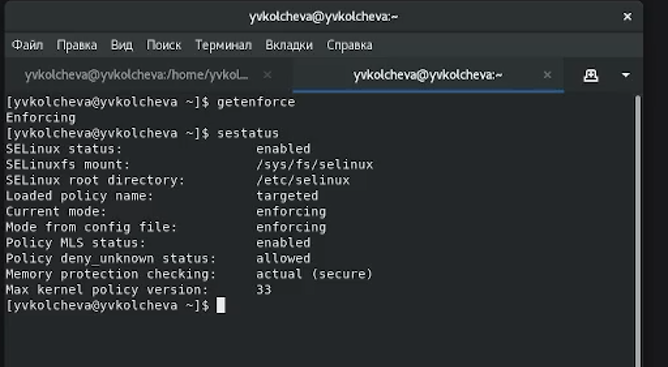


Figure 1: Ввод команд

Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает с помощью команды “service httpd status” (рис. 2)

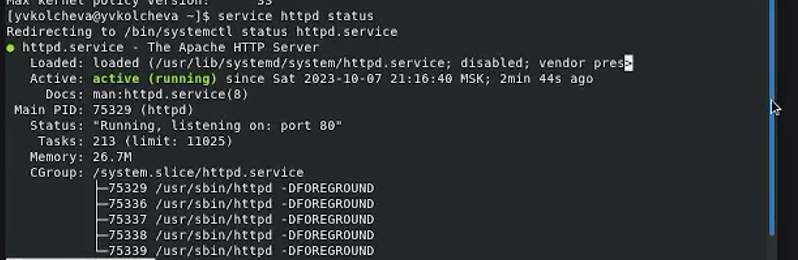


Figure 2: Обращение к веб-серверу

С помощью команды “ps auxZ | grep httpd” определила контекст безопасности веб-сервера Apache - httpd\_t (рис. 3)

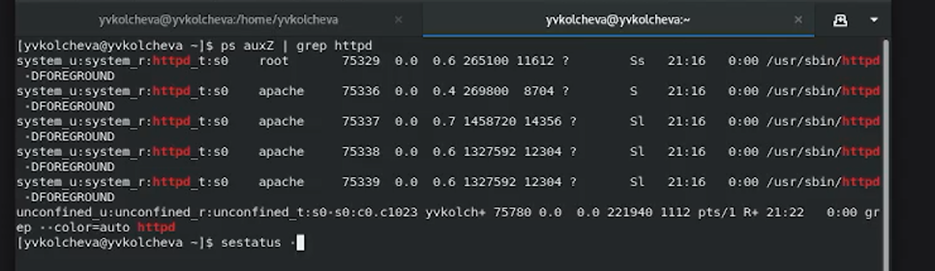


Figure 3: Контекст безопасности

Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды “sestatus -bigrep httpd”. Посмотрела статистику по политике с помощью команды “seinfo”. Множество пользователей - 8, ролей - 14, типов 4995 (рис. 4)

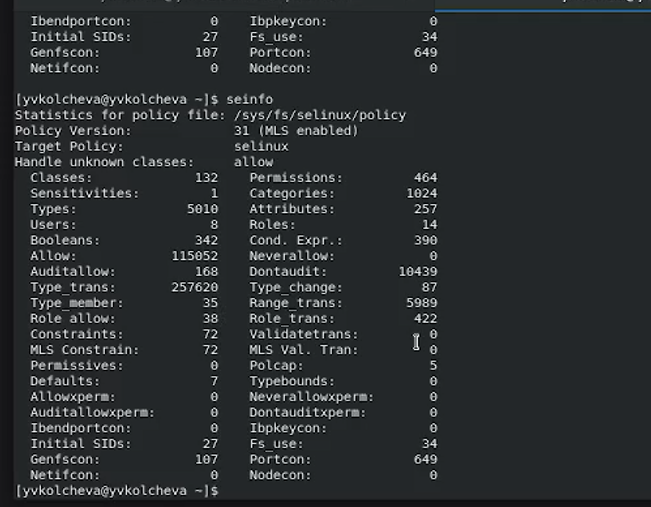


Figure 4: Состояние

С помощью команды “ls -lZ /var/www” посмотрела файлы и поддиректории, находящиеся в директории /var/www. Используя команду “ls -lZ /var/www/html”, определила, что в данной директории файлов нет. Только владелец/суперпользователь может создавать файлы в директории /var/www/html (рис. 5)

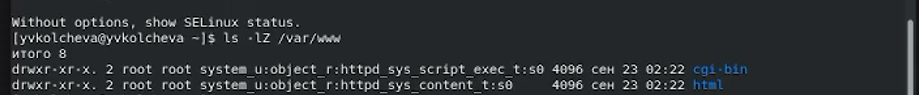


Figure 5: Просмотр

От имени суперпользователя создала html-файл /var/www/html/test.html. Контекст созданного файла - httpd\_sys\_content\_t (рис. 7)

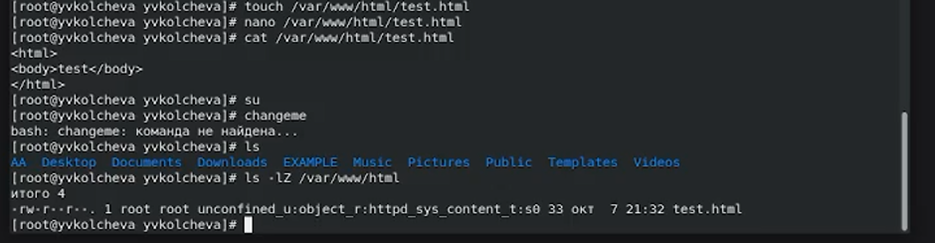


Figure 6: Создание и написание

Обратилась к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”. Файл был успешно отображен (рис. 8)

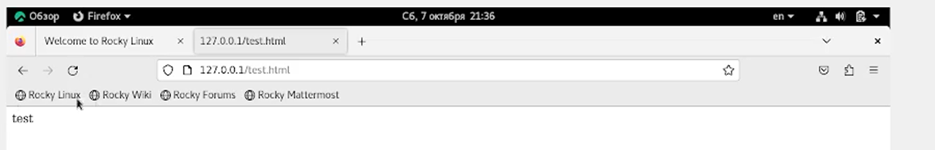


Figure 7: Обращение

Изучив справку man httpd\_selinux, выяснила, что для httpd определены следующие контексты файлов: httpd\_sys\_content\_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. Контекст моего файла - httpd\_sys\_content\_t (в таком случае содержимое должно быть доступно для всех скриптов httpd и для самого демона). Изменила контекст файла на samba\_share\_t командой “sudo chcon -t samba\_share\_t /var/www/html/test.html” и проверила, что контекст поменялся (рис. 8)

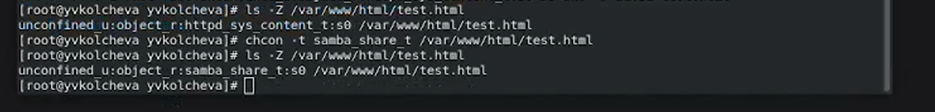


Figure 8: Просмотр

Попробовала еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html” и получила сообщение об ошибке (т.к. к установленному ранее контексту процесс httpd не имеет доступа) (рис. 9)



Figure 9: Ошибка

Командой “ls -l /var/www/html/test.html” убедилась, что читать данный файл может любой пользователь. Просмотрела системный лог-файл веб-сервера Apache командой “sudo tail /var/log/messages”, отображающий ошибки (рис. 10)

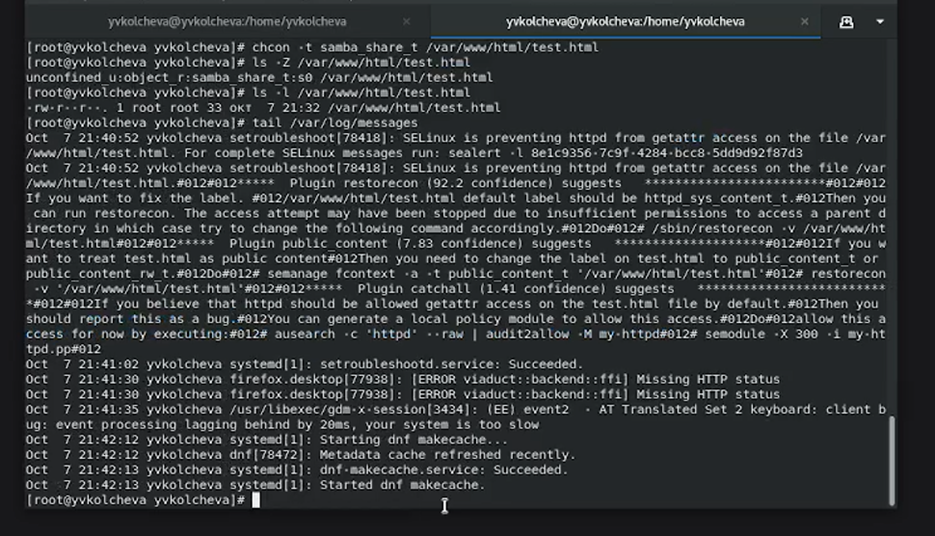


Figure 10: Работа с консолью

В файле /etc/httpd/conf/httpd.conf заменила строчку “Listen 80” на “Listen 81”, чтобы установить веб-сервер Apache на прослушивание TCP-порта 81 (рис. 11)

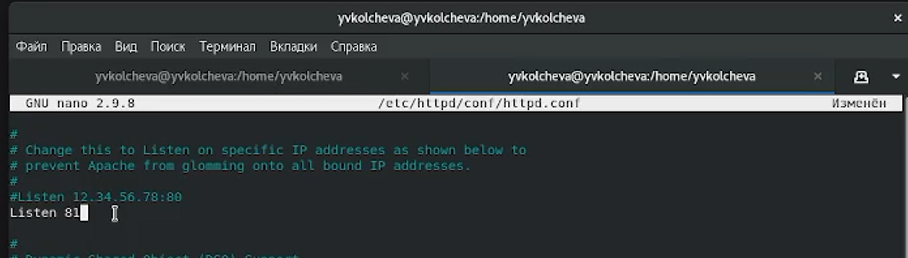


Figure 11: Замена строки

Перезапускаем веб-сервер Apache и анализируем лог-файлы командой “tail -nl /var/log/messages” 12)

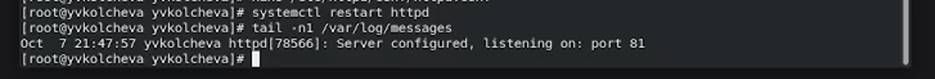


Figure 12: Перезапуск

Просмотрела файлы “var/log/http/error\_log”, “/var/log/http/access\_log” и “/var/log/audit/audit.log” и выяснила, что запись появилась в последнем файле (рис. 13)

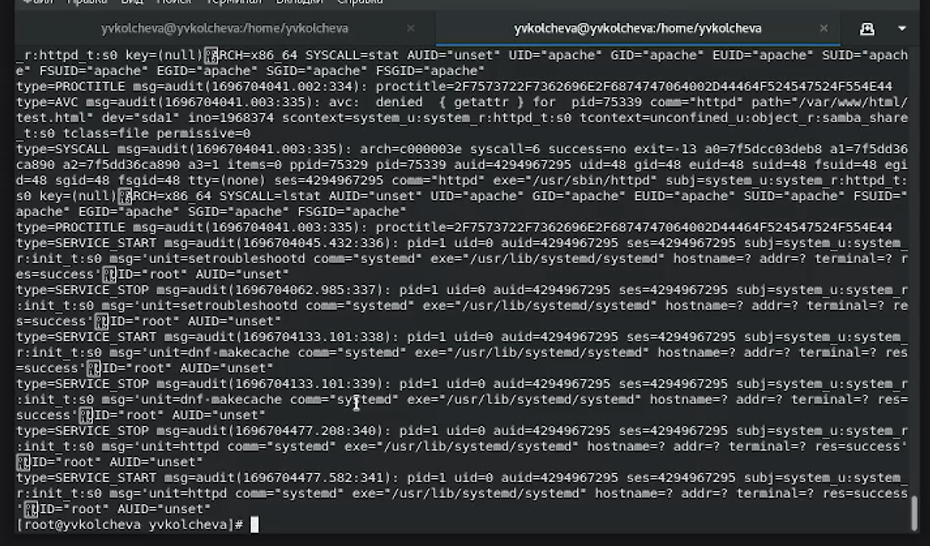


Figure 13: Содержание файла

Выполнила команду “semanage port -a -t http\_port\_t -р tcp 81” и убедилась, что порт TCP-81 установлен. Проверила список портов командой “semanage port -l | grep http\_port\_t”, убедилась, что порт 81 есть в списке и запускаем веб-сервер Apache снова (рис. 14)



Figure 14: Работа с консолью

Вернула контекст “httpd\_sys\_cоntent\_t” файлу “/var/www/html/test.html” командой “chcon -t httpd\_sys\_content\_t /var/www/html/test.html” (рис. 3.16) и после этого попробовала получить доступ к файлу через веб-сервер, введя адрес “http://127.0.0.1:81/test.html”, в результате чего увидела содежимое файла - слово “test” (рис. 15)(рис. 16)



Figure 15: Возвращение

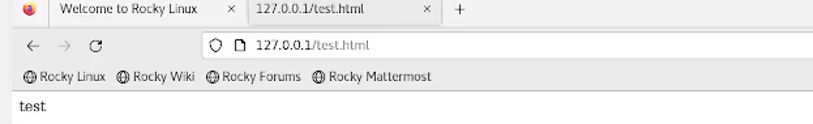


Figure 16: Содержимое файла

Исправила обратно конфигурационный файл apache, вернув “Listen 80”. Попыталась удалить привязку http\_port к 81 порту командой “semanage port -d -t http\_port\_t -p tcp 81”, но этот порт определен на уровне политики, поэтому его нельзя удалить (рис. 17)

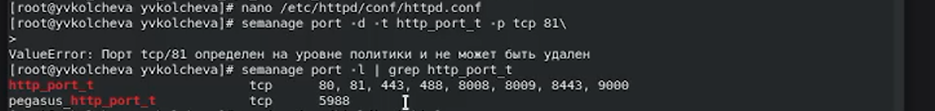


Figure 17: Попытка удаления

Удалила файл “/var/www/html/test.html” командой “rm /var/www/html/test.html” (рис. 17)

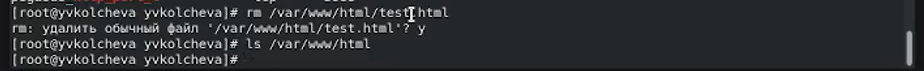


Figure 18: Удаление файла

# Выводы

В ходе выполнения данной лабораторной работы я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux и проверила работу SELinux на практике совместно с веб-сервером Apache.

# Список литературы

Лабораторная работа №6

SELinux – описание и особенности работы с системой [Электронный ресурс]. URL: https://habr.com/ru/company/kingservers/blog/209644/.