Лабораторная работа №6

Мандатное разграничение прав в Linux

Липатникова М.С. группа НФИбд-02-19

Содержание

# 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

Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью ко- манд: getenforce и sestatus. Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает: service httpd status (fig. 1).

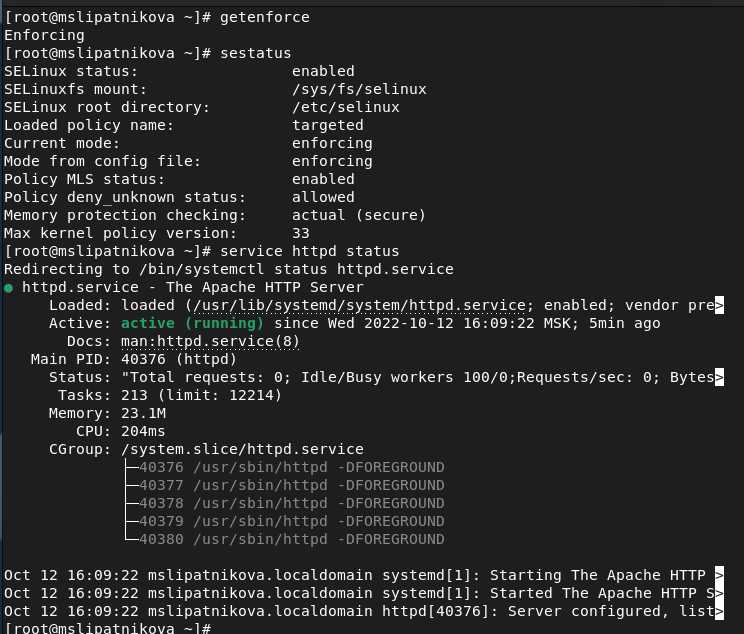


Figure 1: Проверка SELinux

Нашла веб-сервер Apache в списке процессов, его контекст безопасности: httpd\_t (ps -eZ | grep httpd)(fig. 2).

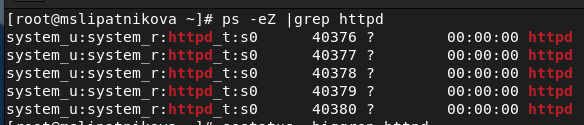


Figure 2: Список процессов: веб-сервер Apache

Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды: sestatus -b | grep httpd. Обратила внимание, что многие из них находятся в положении «off»(fig. 3).

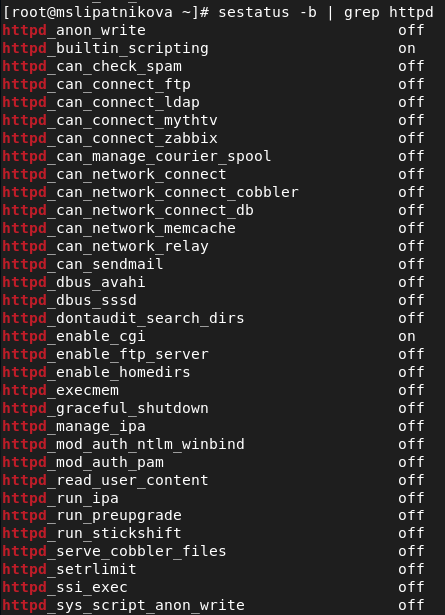


Figure 3: Переключатели для Apache

Посмотрела статистику по политике с помощью команды seinfo, также определила множество пользователей (8), ролей (14), типов (5002) (fig. 4).



Figure 4: Статистика по политике

Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды: ls -lZ /var/www. Определила тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html (root). Создала от имени суперпользователя html-файл - /var/www/html/test.html, чтобы на странице выводилось слово test. Проверила контекст созданного мной файла (httpd\_sys\_content\_t). Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедилась, что файл был успешно отображён (fig. 5).

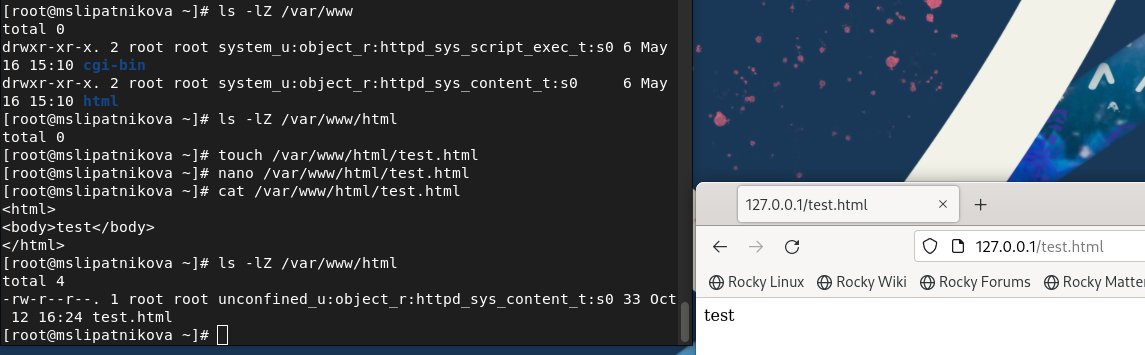


Figure 5: Работа в директории /var/www/html

Изучила справку man httpd\_selinux и выяснила, какие контексты файлов определены для httpd. Совпадают с типом файла test.html. Тип httpd\_sys\_content\_t позволяет процессу httpd получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.

Изменила контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на (к которому процесс httpd не должен иметь доступа) samba\_share\_t:

chcon -t samba\_share\_t /var/www/html/test.html

ls -Z /var/www/html/test.html

Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получила сообщение об ошибке: Forbidden. You don’t have permission to access /test.html on this server (fig. 6).

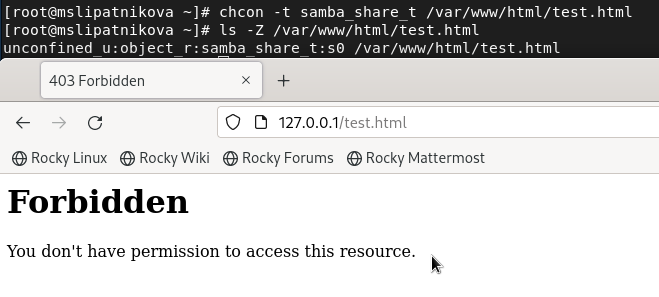


Figure 6: Изменение контекста

Файл не был отображён, хотя права доступа позволяют читать этот файл любому пользователю: ls -l /var/www/html/test.html. Это произошло, т.к. мы изменили контекст к которому процесс httpd не должен иметь доступа. Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл: tail /var/log/messages (fig. 7).

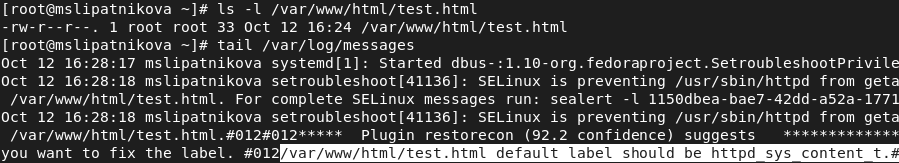


Figure 7: Файл ошибок

Попробовала 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 нашла строчку Listen 80 и заменила её на Listen 81 (fig. 8). Выполнила перезапуск веб-сервера Apache. Сбоя не произошло. Проанализировала лог-файлы: tail -nl /var/log/messages (fig. 9).

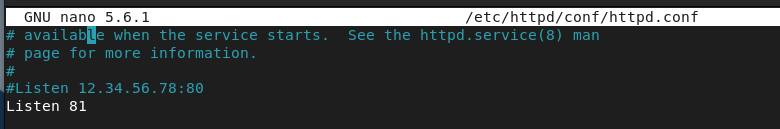


Figure 8: Замена 80-81

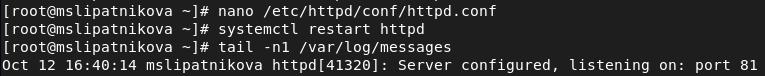


Figure 9: Перезапуск сервера

Выполнила команду: semanage port -a -t http\_port\_t -р tcp 81 (уже существует). После этого проверьте список портов командой: semanage port -l | grep http\_port\_t Порт 81 есть в списке. Попробовала запустить веб-сервер Apache ещё раз. Сбоя также нет (fig. 10).

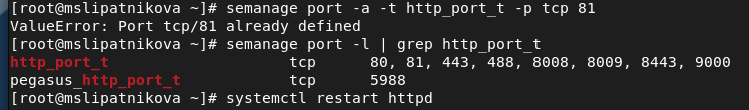


Figure 10: Перезапуск сервера

Вернула контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html: chcon -t httpd\_sys\_content\_t /var/www/html/test.html. После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Можно увидеть содержимое файла — слово «test» (fig. 11).

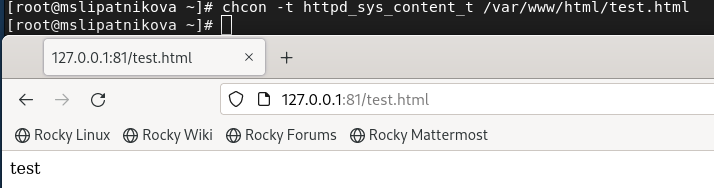


Figure 11: Перезапуск сервера - работает

Исправила обратно конфигурационный файл apache, вернув Listen 80(fig. 12).

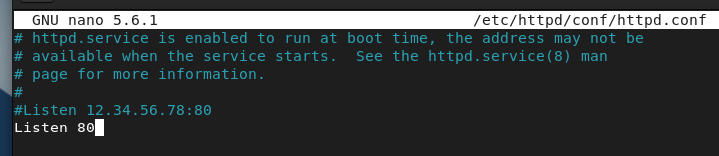


Figure 12: Замена 81-80

Удалить привязку http\_port\_t к 81 порту (semanage port -d -t http\_port\_t -p tcp 81) не получилось, не позволяется. Удалила файл /var/www/html/test.html: rm /var/www/html/test.html(fig. 13).

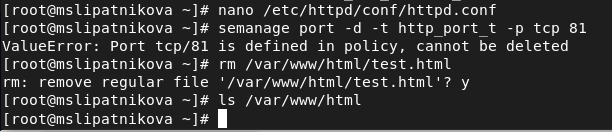


Figure 13: Удаление

# 3 Вывод

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinx на практике совместно с веб-сервером Apache.

# 4 Список литературы

1. Теоретические материалы курса.