Мандатное разграничение прав в Linux

Лабораторная работа №6

Тарутина Кристина Олеговна

Содержание

Список иллюстраций

Список таблиц

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

Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: service httpd status Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www

(рис. 2.1).

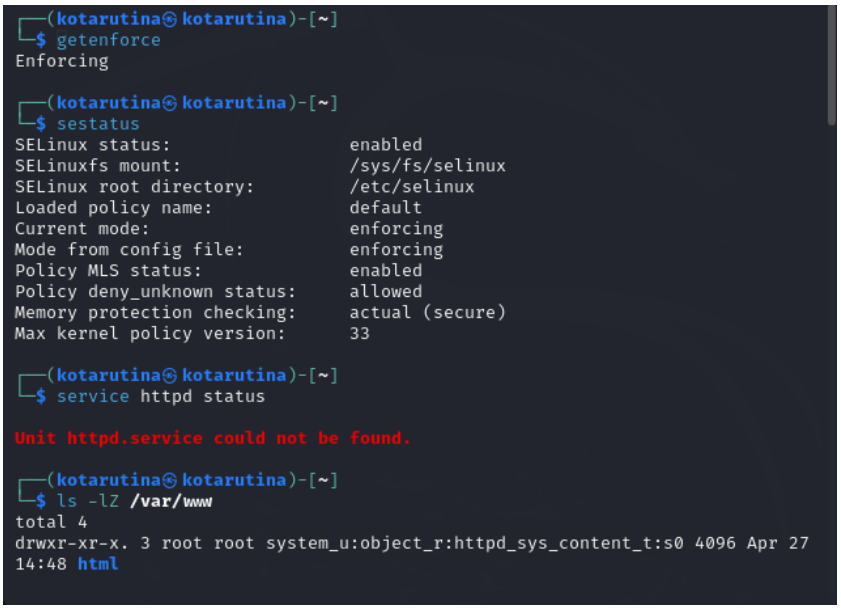

Рис. 2.1: Название рисунка

Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html (рис. 2.2).

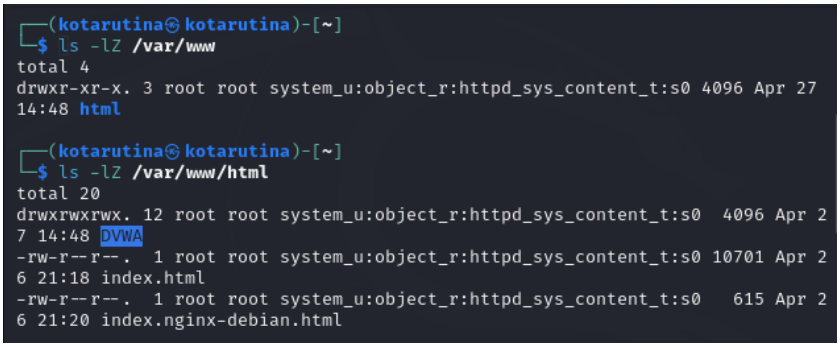

Рис. 2.2: Название рисунка

Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

test

(рис. 2.3).

Рис. 2.3: Название рисунка

Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён Тут, к сожалению, по какой-то причине у меня отказался запускаться firefox (рис. 2.4).

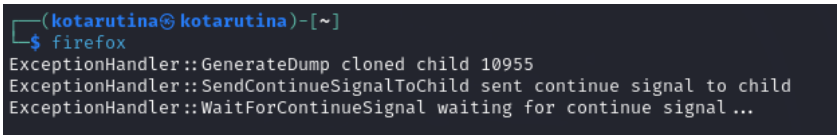

Рис. 2.4: Название рисунка

Изучите справку man httpd_selinux и выясните, какие контексты файлов определены для httpd. Сопоставьте их с типом файла test.html. Проверить контекст файла можно командой ls -Z. ls -Z /var/www/html/test.html Измените 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: chcon -t samba_share_t /var/www/html/test.html ls -Z /var/www/html/test.html (рис. 2.5).

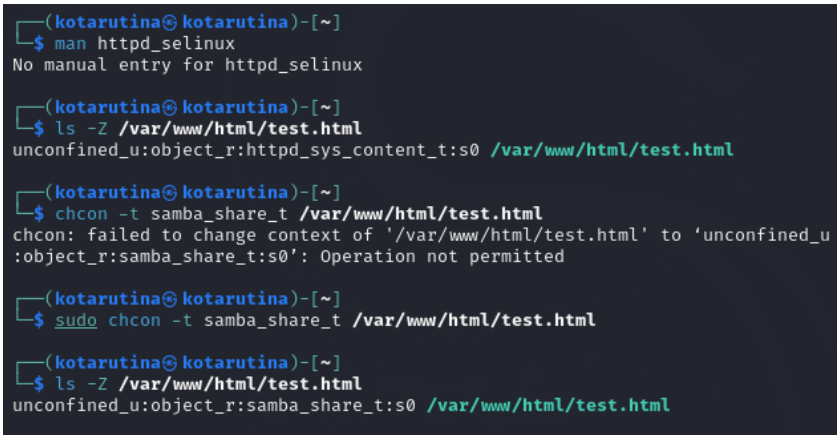

Рис. 2.5: Название рисунка

Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? ls -l /var/www/html/test.html Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: tail /var/log/messages Если в системе окажутся запущенными процессы setroubleshootd и audtd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log. Проверьте это утверждение самостоятельно. (рис. 2.6).

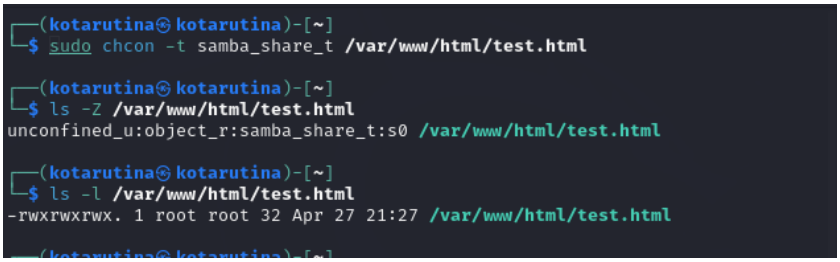

Рис. 2.6: Название рисунка

Проанализируйте лог-файлы: tail -nl /var/log/messages Просмотрите файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log и выясните, в каких файлах появились записи. Выполните команду semanage port -a

-t http_port_t -p tcp 81 После этого проверьте список портов командой semanage port -l | grep http_port_t Убедитесь, что порт 81 появился в списке. Попробуйте запустить веб-сервер Apache ещё (рис. 2.7).

Рис. 2.7: Название рисунка

Верните контекст httpd_sys_content__t к файлу /var/www/html/ test.html: chcon -t httpd_sys_content_t /var/www/html/test.html После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Вы должны увидеть содержимое файла — слово «test». Исправьте обратно конфигурационный файл apache, вернув Listen 80. Удалите привязку http_port_t к 81 порту: semanage port -d -t http_port_t -p tcp 81 и проверьте, что порт 81 удалён. Удалите файл /var/www/html/test.html: rm /var/www/html/test.html (рис. 2.8).

Рис. 2.8: Название рисунка

3 Выводы

Мы успешно развили навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux

Проверили работу SELinx на практике совместно с веб-сервером Apache.

Список литературы