Информационная безопасность. Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Терентьев Егор Дмитриевич 1032192875

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

Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus. fig. 1.

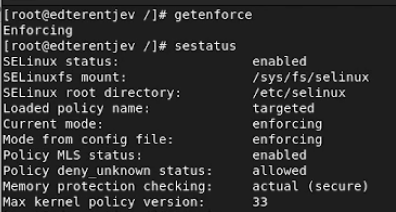


Figure 1: getenforce

Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает fig. 2.

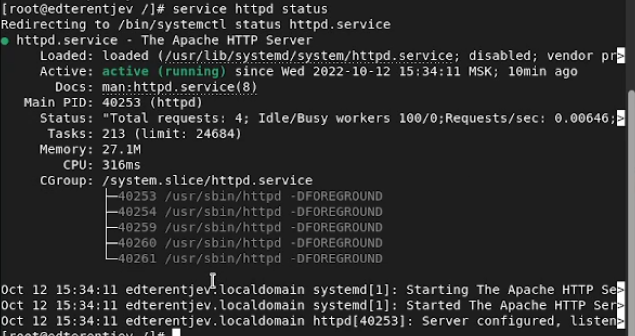


Figure 2: service\_httpd\_status

Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт: system\_u:system\_r:httpd\_t:s0 fig. 3.

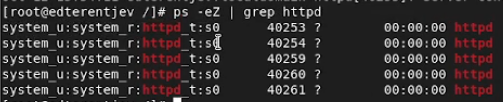


Figure 3: ps\_auxz\_httpd

Посмотрите текущее состояние переключателей SELinux для Apache fig. 4

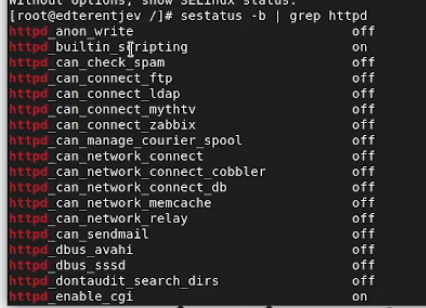


Figure 4: sestatus\_httpd

Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов. fig. 5

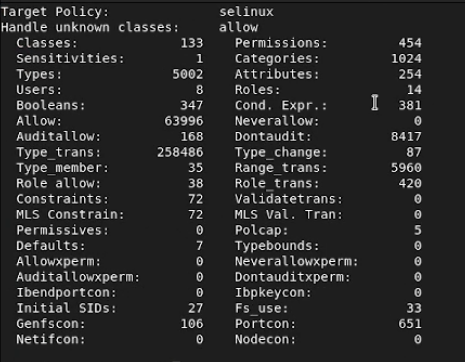


Figure 5: seinfo

Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html fig. 6.

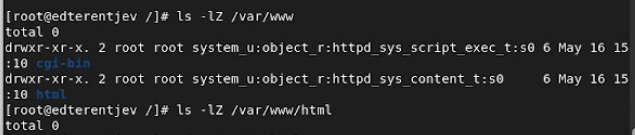


Figure 6: ls\_lz

Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл fig. 7.

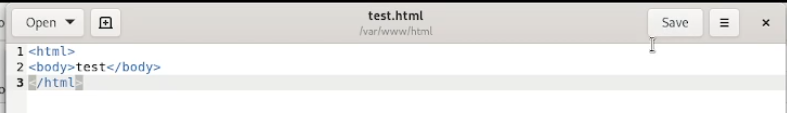


Figure 7: html\_file

Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён. fig. 8

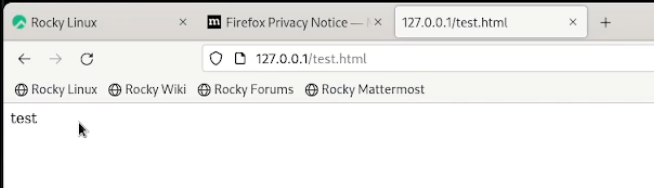


Figure 8: test\_file\_on\_site

Проверить контекст файла. 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 fig. 9.

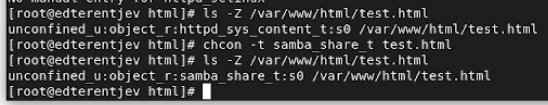


Figure 9: samba\_share\_t

Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Вы должны получить сообщение об ошибке fig. 10.

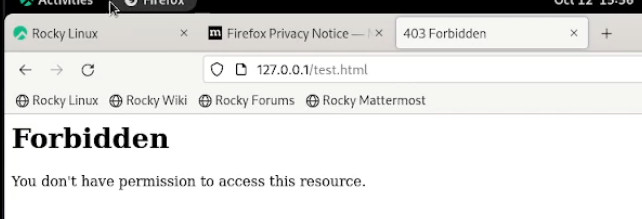


Figure 10: error

ls -l /var/www/html/test.html Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: tail /var/log/messages fig. 11.

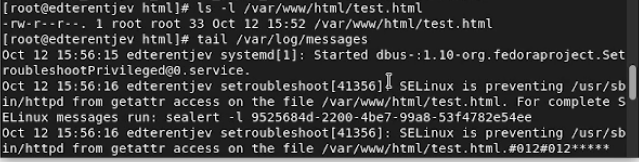


Figure 11: logs

Попробуйте запустить веб-сервер Apache на прослушивание ТСР-порта 81. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Проанализируйте лог-файлы. fig. 12

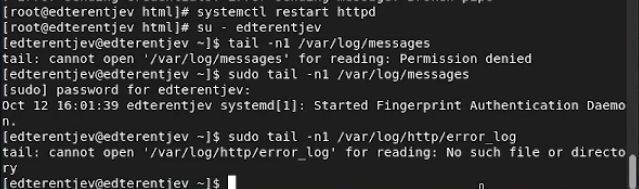


Figure 12: restart\_log

Выполните команду semanage port -a -t http\_port\_t -р tcp 81 После этого проверьте список портов командой semanage port -l | grep http\_port\_t Убедитесь, что порт 81 появился в списке. fig. 13

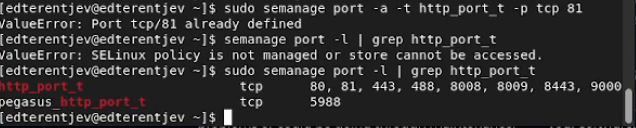


Figure 13: semanage\_port

Верните контекст httpd\_sys\_cоntent\_t к файлу /var/www/html/ test.html fig. 14

Figure 14: httpd_sys_cоntent

Figure 14: httpd\_sys\_cоntent

Удалите привязку http\_port\_t к 81 порту и проверьте, что порт 81 удалён. (Удалить привязку невозможно) Удалите файл /var/www/html/test.html fig. 15

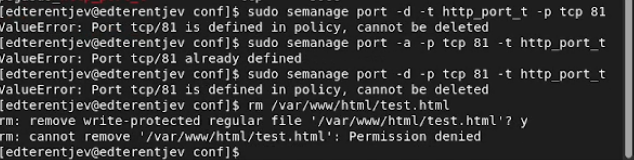


Figure 15: semanage\_rm

# 3 Выводы

В результате выполнения работы я развитл навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux, а также проверил работу SELinx на практике совместно с веб-сервером Apache.

# 4 Список литературы

1. Методические материалы курса