Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Виктория Михайловна Шутенко

Содержание

# Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Подготовка к выполнению лабораторной работы №6

Сначала я выполнила подготовительные действия для стенда лабораторной работы №6:

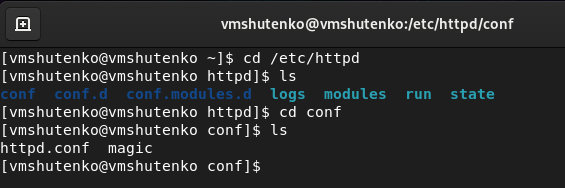


Figure 1: Установка httpd.

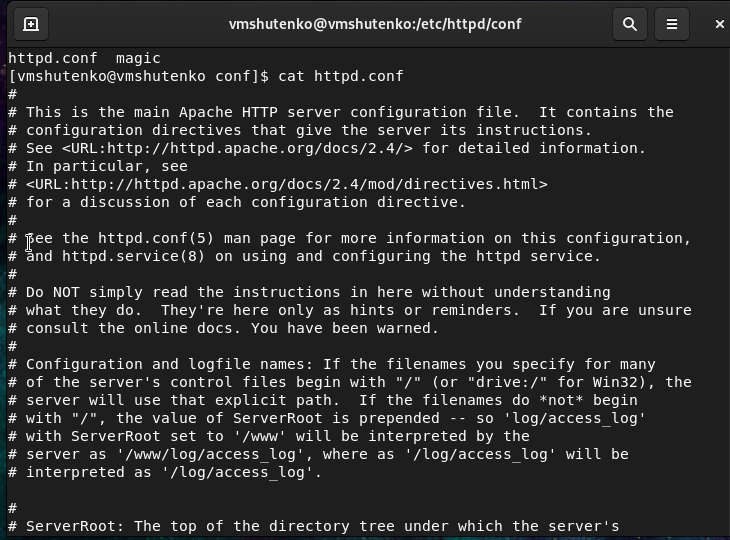


Figure 2: Файл httpd.conf.

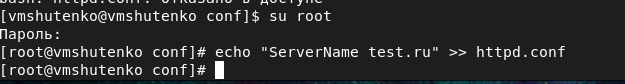


Figure 3: Задание параметра ServerName

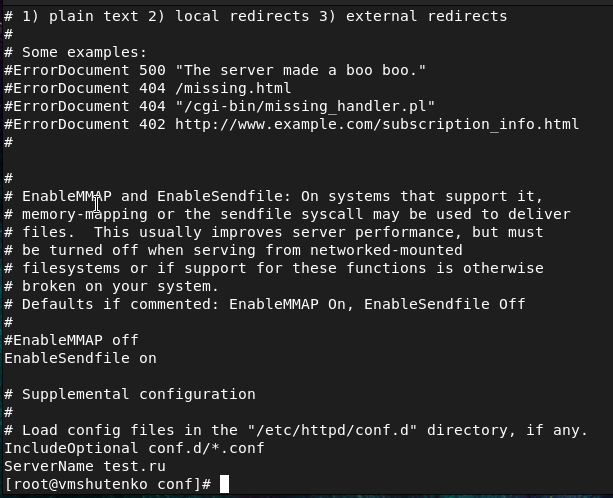


Figure 4: Проверка наличия параметра ServerName

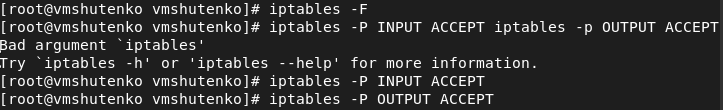


Figure 5: Отключение пакетного фильтра.

# Ход работы

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

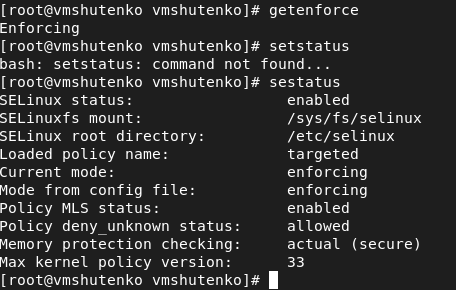


Figure 6: Проверка работоспособности SELinux.

1. Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает:

service httpd status

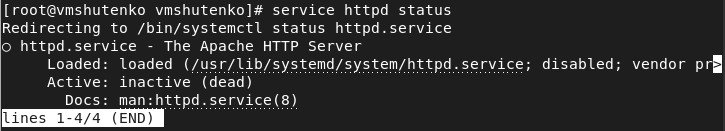


Figure 7: Обращение к веб-серверу.

1. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности, используя команду

ps auxZ | grep httpd

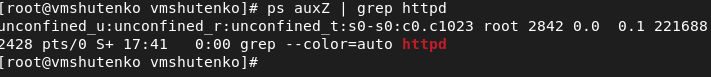


Figure 8: Определение контекста безопасности.

1. Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды

sestatus -bigrep httpd

Обратила внимание, что многие из них находятся в положении «off».

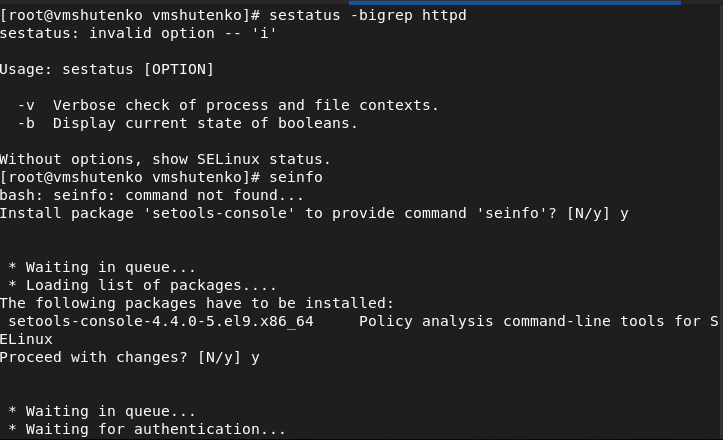


Figure 9: Определение текущего состояния переключателей SELinux.

1. Посмотрела статистику по политике с помощью команды seinfo, определила множество пользователей, ролей, типов.

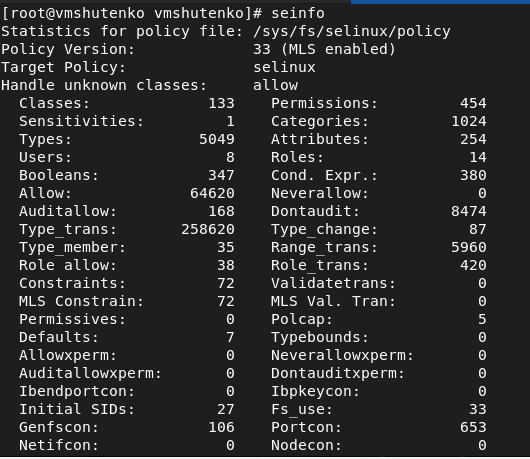


Figure 10: Статистика по политике.

1. Определила тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды

ls -lZ /var/www

1. Определила тип файлов, находящихся в директории /var/www/html:

ls -lZ /var/www/html

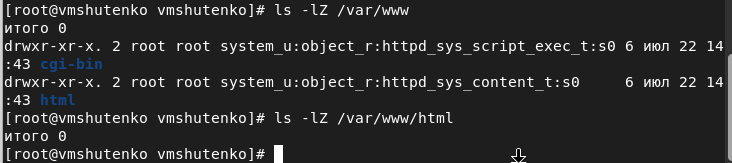


Figure 11: Определение типов файлов и поддиректорий.

1. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html.

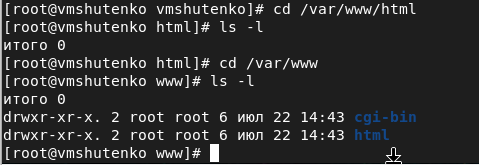


Figure 12: Определение круга пользователей.

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

<html>  
<body>test</body>  
</html>

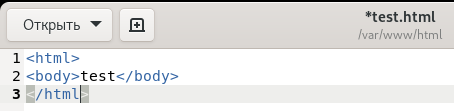


Figure 13: Файл test.html.

1. Проверила контекст созданного мною файла.
2. Обратилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html.
3. Изучила справку man httpd\_selinux. Сопоставьте их с типом файла test.html. Проверила контекст файла командой ls -Z.

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

1. Изменила 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

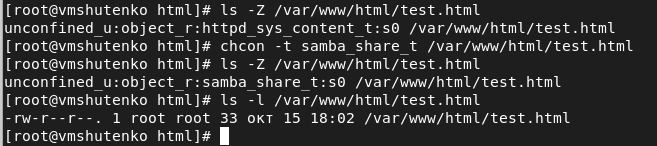


Figure 14: Проверка, изменение и просмотр контекста.

1. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html.
2. Проанализировала ситуацию.

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

Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл:

tail /var/log/messages

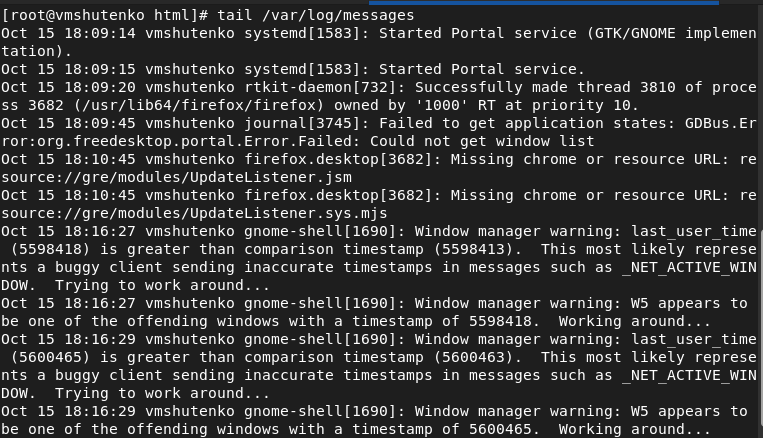


Figure 15: Cистемный лог-файл.

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.

1. 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 замените её на Listen 81.

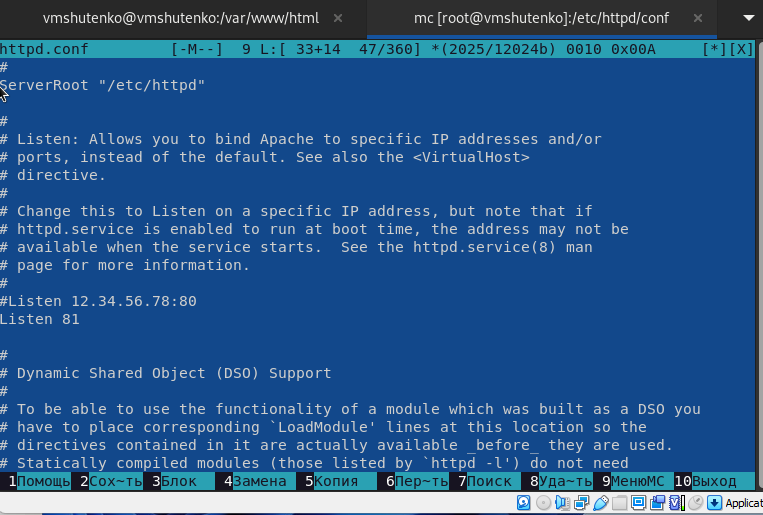


Figure 16: Изменение Listen 80 на Listen 81 в файле httpd.conf.

1. Выполнила перезапуск веб-сервера Apache.
2. Проанализировала лог-файлы:

tail -nl /var/log/messages

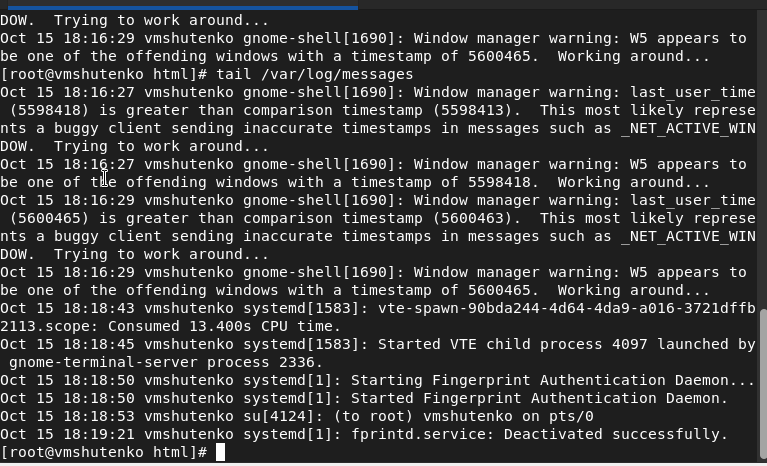


Figure 17: Cистемный лог-файл.

Просмотрела файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log

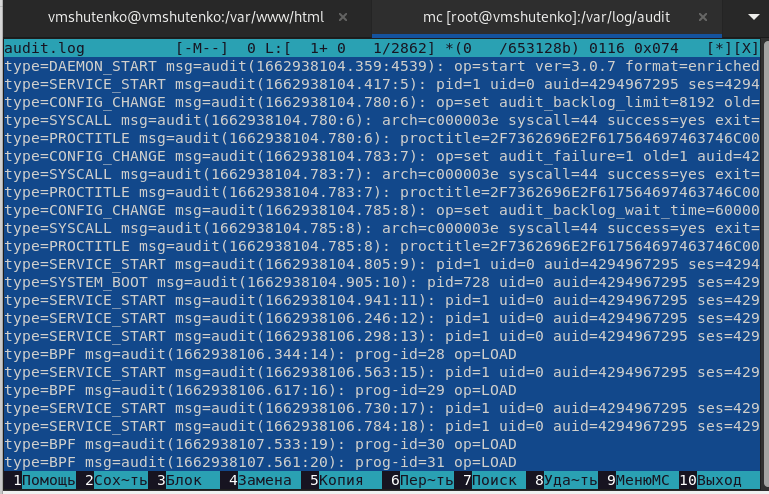


Figure 18: Лог-файл audit.log.

1. Выполнила команду

semanage port -a -t http\_port\_t -р tcp 81

После этого проверила список портов командой

semanage port -l | grep http\_port\_t

Убедилась, что порт 81 появился в списке.

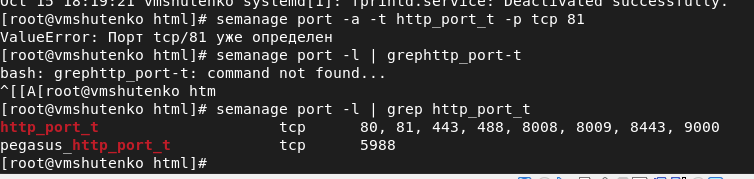


Figure 19: Добавление порта 81.

1. Попробовала запустить веб-сервер Apache ещё раз.
2. 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.

1. Исправила обратно конфигурационный файл apache, вернув Listen 80.
2. Удалила привязку http\_port\_t к 81 порту:

semanage port -d -t http\_port\_t -p tcp 81

1. Удалила файл /var/www/html/test.html:

rm /var/www/html/test.html

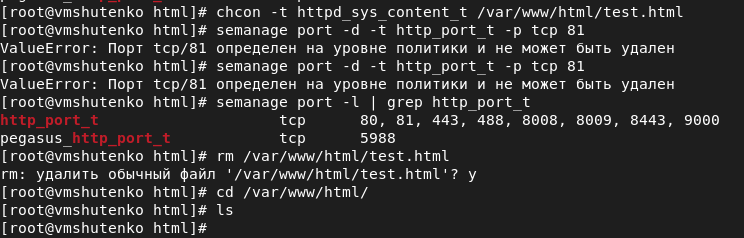


Figure 20: Возвращение контекста, удаление привязки к порту 81 и удаление файла test.html.