Лабораторная работа № 6. Мандаторное разграничение прав в Linux.

Лёшьен Стефани, НФИбд-02-19

Содержание

# 1 Цель работы

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

# 2 Последовательность выполнения работы

1. От имени пользователя root установили веб-сервер Apache c помощью команды yum install httpd.

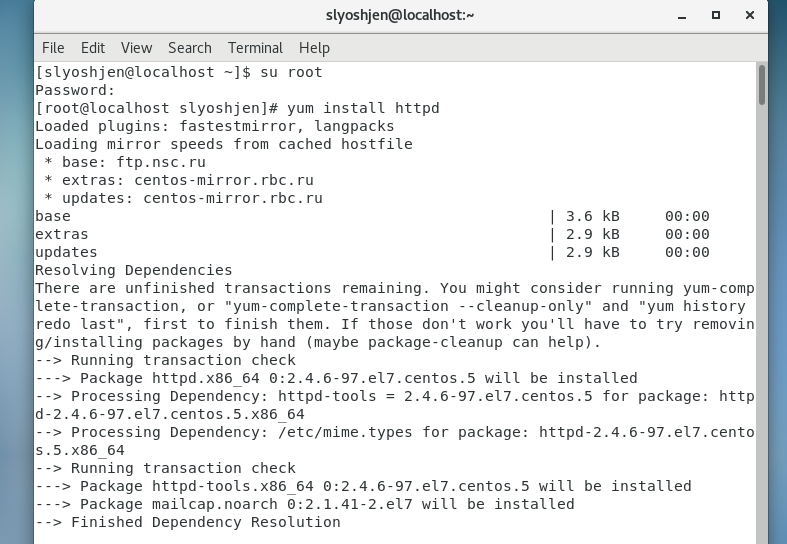


Figure 1: Установка веб-сервер Apache

1. В конфигурационном файле /etc/httpd/httpd.conf задали параметр ServerName: ServerName test.ru Для чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе. Также отключили пакетный фильтр командами : iptables -F iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT

* Убедились, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.

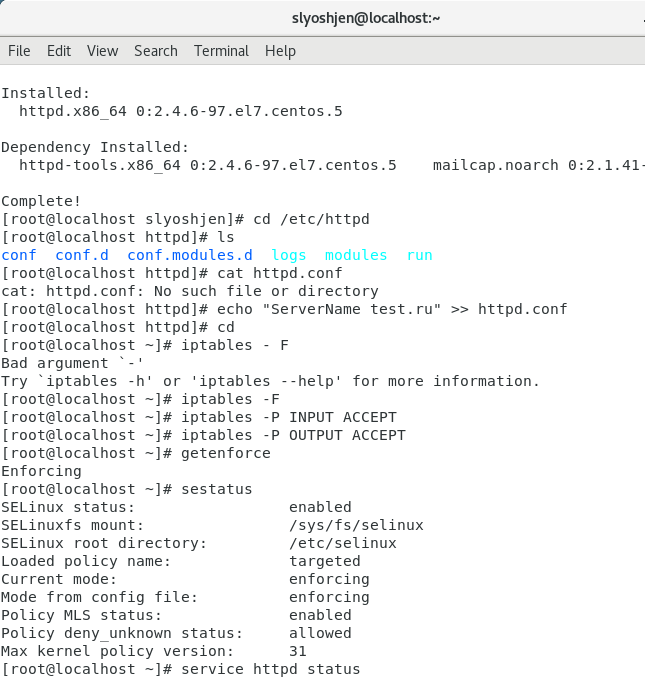


Figure 2: Отключили пакетный фильтр

1. Обратились с помощью браузера к веб-серверу, запущенному на компьютере, и убедились, что последний работает: service httpd start

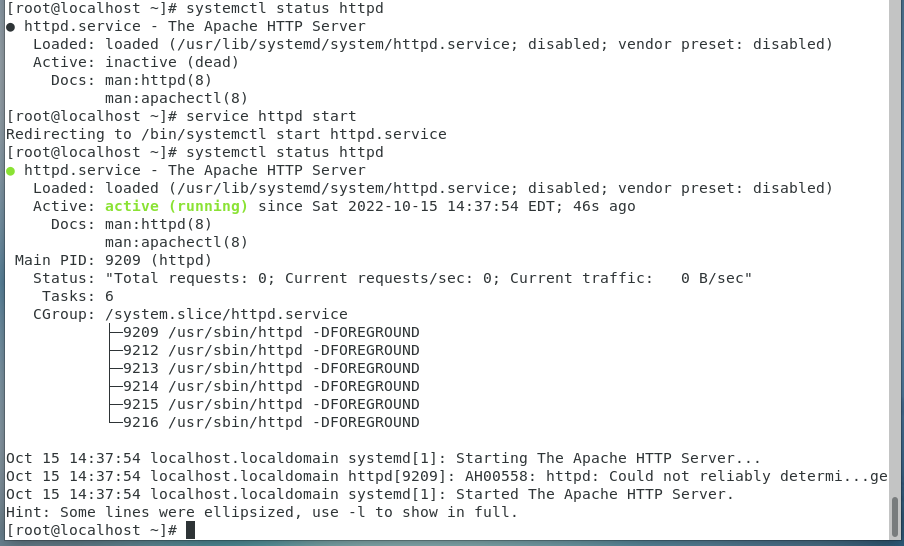


Figure 3: service httpd start

1. Нашли веб-сервер Apache в списке процессов : ps auxZ | grep httpd или ps -eZ | grep httpd. Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды sestatus -bigrep httpd Многие переключателей находятся в положении «off»

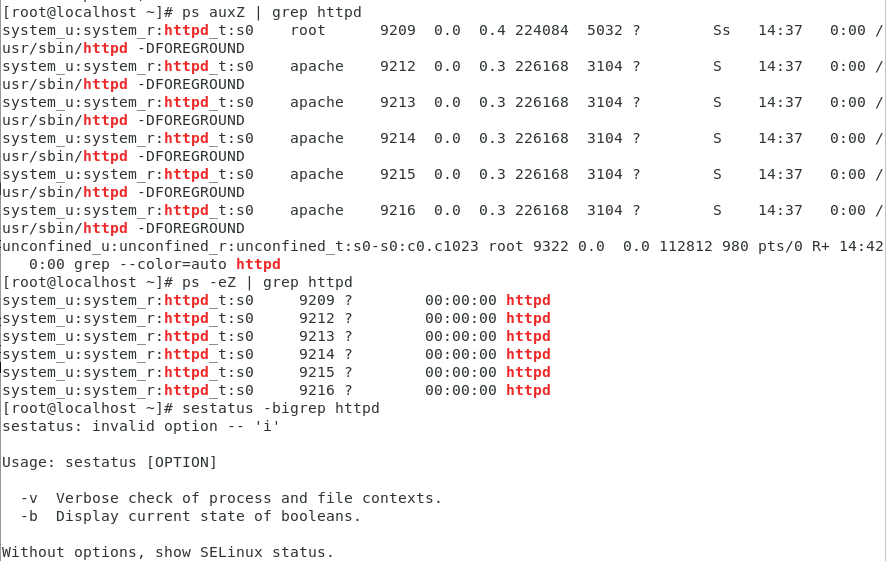


Figure 4: Нашли веб-сервер Apache в списке процессов

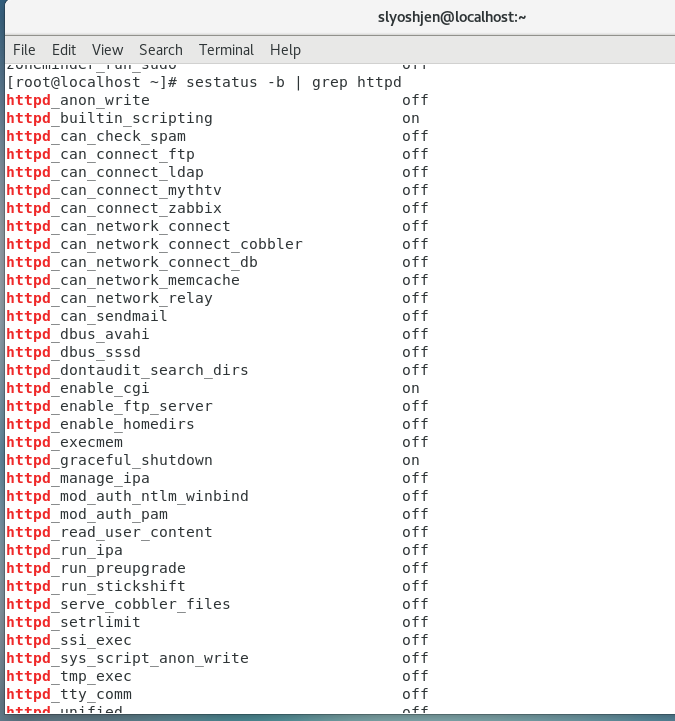


Figure 5: Многие переключателей находятся в положении «off»

1. Определили тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www и определили тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html. Создали от имени суперпользователя html-файл /var/www/html/test.html следующего содержания:

* test

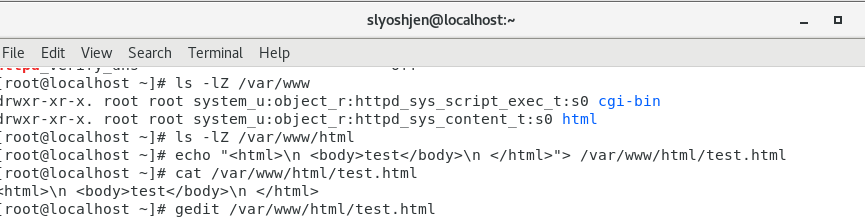


Figure 6: Создали от имени суперпользователя html-файл

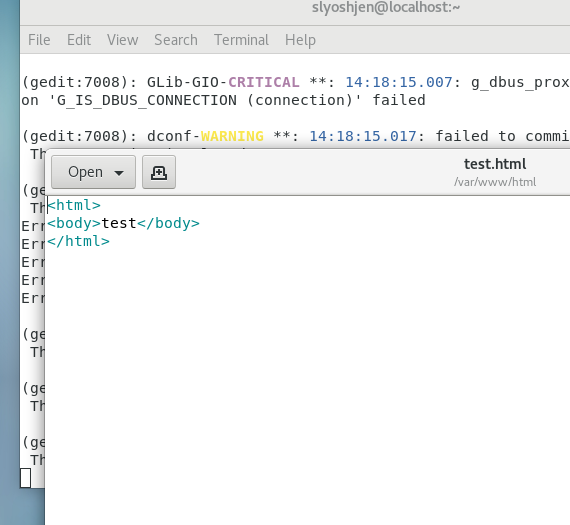


Figure 7: html-файл test.html

1. Обратились к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Файл успешно отображён.

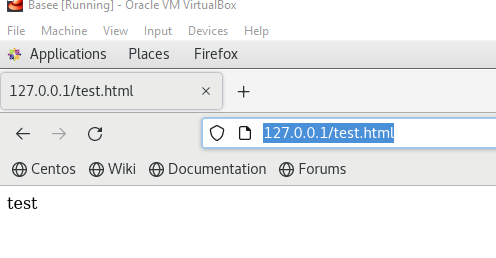


Figure 8: html-файл в веб-сервер

1. Проверили контекст файла можно командой ls -Z. Изменили 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.

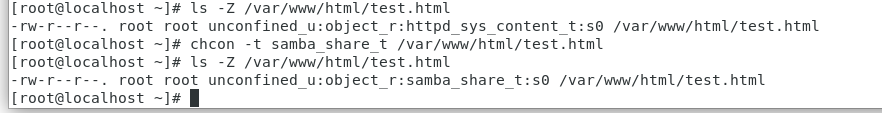


Figure 9: Изменили контекст файла на samba\_share\_t

1. Попробовали ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Мы получили сообщение об ошибке.
2. Просмотрели системный лог-файл tail /var/log/messages и выполнили команду : semanage port -a -t http\_port\_t -р tcp 81 После этого проверили список портов командой: semanage port -l | grep http\_port\_t Порт 81 появился в списке.



Figure 10: Проверили список портов

1. Вернули контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html. После этого мы получили доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Мы увидели содержимое файла — слово «test».
2. Удалили привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и проверили, что порт 81 удалён. Удалили файл /var/www/html/test.html

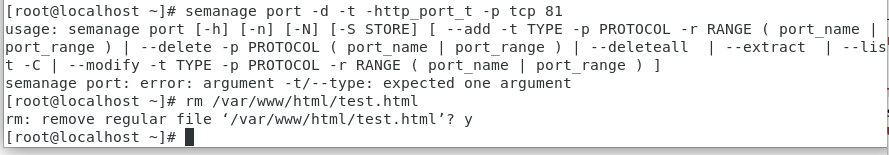


Figure 11: Удалили файл /var/www/html/test.html

# 3 Выводы

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.

# 4 Библиография

1. Методические материалы курса