Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Голощапова Ирина Борисовна

Содержание

# 1 Цели и задачи лабораторной работы

## 1.1 Цели и задачи работы

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

# 2 Выполнение лабораторной работы

## 2.1 Подготовка к выполнению работы

1. Установила от имени администратора httpd (рис. [1](#fig:01))

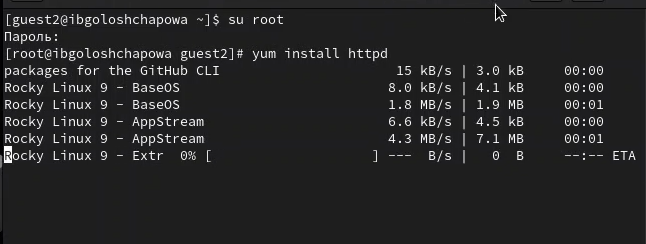


Figure 1: Установка httpd

1. В конфигурационном файле /etc/httpd/httpd.conf задала параметр ServerName (рис. [2](#fig:02)):

Figure 2: параметр ServerName

Figure 2: параметр ServerName

1. Также проследила, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp (рис. [3](#fig:03)):

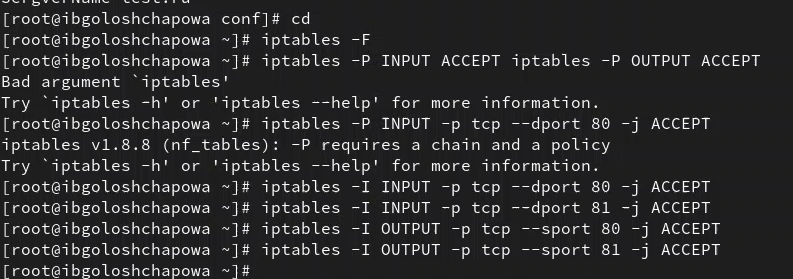


Figure 3: Отключение пакетного фильтра

## 2.2 Выполнение основной части работы

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted (рис. [4](#fig:04)):

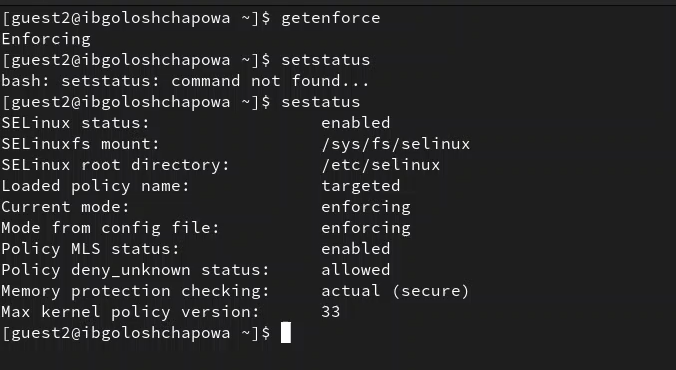


Figure 4: Вход в систему

1. Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает (рис. [5](#fig:05)):

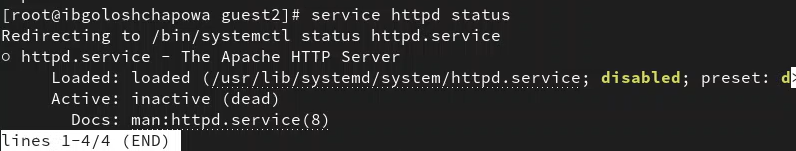


Figure 5: Обращение к веб-браузеру

1. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности (рис. [6](#fig:06)):

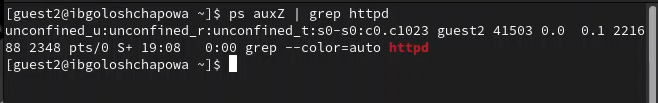


Figure 6: Apach

1. Посмотрела текущее состояние переключателей SELinux для Apache (рис. [7](#fig:07)):

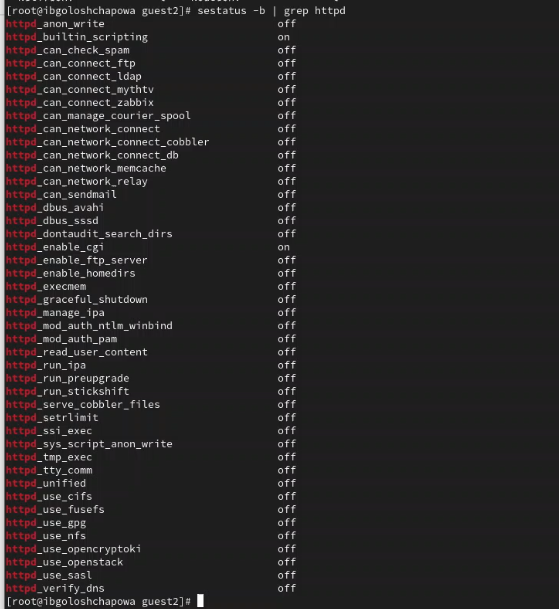


Figure 7: переключатели SELinux

1. Посмотрела статистику по политике с помощью команды seinfo, также определила множество пользователей, ролей, типов (рис. [8](#fig:08)):



Figure 8: seinfo

1. Определила тип файлов и поддиректорий, находящихся в директории /var/www (рис. [9](#fig:09)):

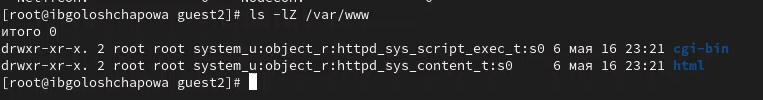


Figure 9: тип файлов и поддиректорий

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 (рис. [10](#fig:10)):

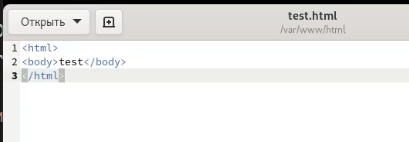


Figure 10: html-файл

1. Обратилаась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html (рис. [11](#fig:11)):

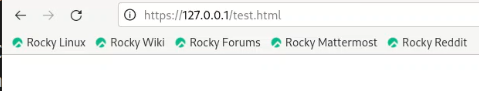


Figure 11: Обращение к файлу через веб-сервер

1. Изучила справку man httpd\_selinux и выяснила, какие контексты файлов определены для httpd. Сопоставила их с типом файла test.html. Проверила контекст файла командой ls -Z (рис. [12](#fig:12)):

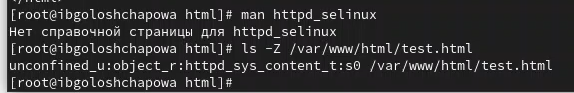


Figure 12: контексты файлов для httpd

1. Изменила контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на другой, к которому процесс httpd не должен иметь доступа, например, на samba\_share\_t (рис. [13](#fig:13)):

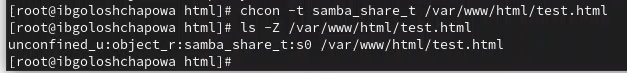


Figure 13: Изменение контекст файла

1. Проанализировала ситуацию. Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл (рис. [14](#fig:14)) (рис. [15](#fig:15)):

Figure 14: log-файлы веб-сервера Apache

Figure 14: log-файлы веб-сервера Apache

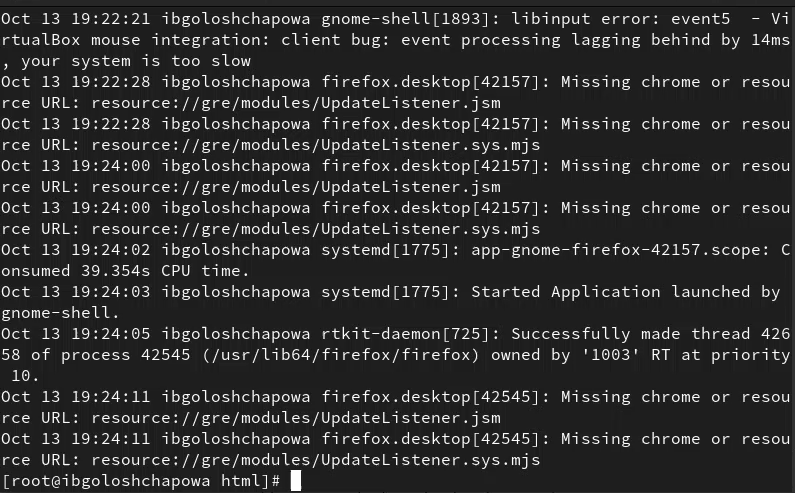


Figure 15: log-файлы веб-сервера Apache\_2

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 найшла строчку Listen 80 и заменила её на Listen 81 (рис. [16](#fig:16)):

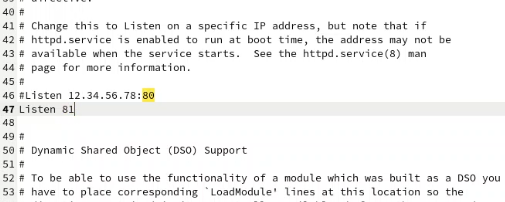


Figure 16: Замена на Listen 81

1. Выполнила команду и после этого проверила список портов(рис. [17](#fig:17)):

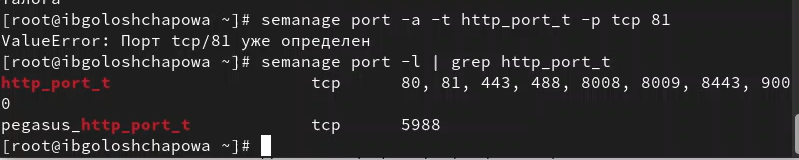


Figure 17: Список портов

1. Вернула контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html и после этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html (рис. [18](#fig:18)):

Figure 18: Возврат контекст

Figure 18: Возврат контекст

1. Исправила обратно конфигурационный файл apache, вернув Listen 80. Удалила привязку http\_port\_t к 81 порту и проверьила, что порт 81 удалён. Затем удалила файл /var/www/html/test.html (рис. [19](#fig:19)):

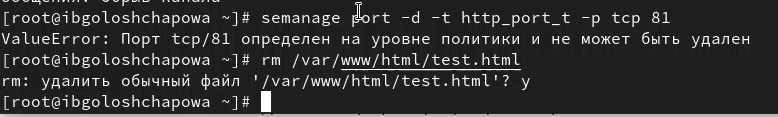


Figure 19: Удаление привязки и файла

# 3 Выводы

В ходе лабораторной работы мне удалось:

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

# 4 Библиография

1. [Git - система контроля версий](https://github.com/)
2. [Rocky Linux](https://rockylinux.org/)