Отчет по лабораторной работе №5

Дискреционное разграничение прав в Linux. Расширенные атрибуты

Низамова Альфия Айдаровна

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 Выполнение

## 2.1 Создание программы

1. Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted (рис.1)
2. Обратимся с помощью браузера к веб-серверу, запущенному на компьютере, и убедимся, что последний работает (рис.1)

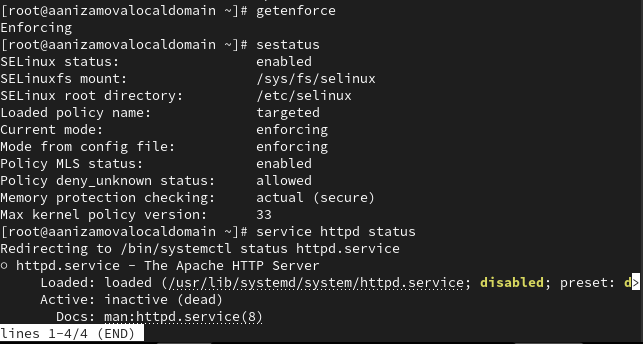


Рис. 1

1. Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности. (рис.2)

Рис. 2

Рис. 2

1. Посмотрим текущее состояние переключателей SELinux для Apache. Многие из них находятся в положении «off» (рис.3)

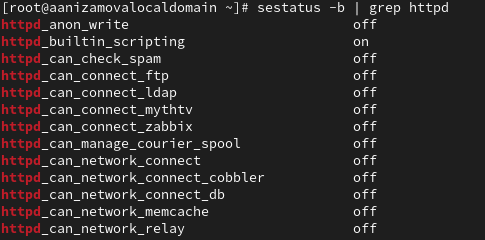


Рис. 3

1. Посмотрим статистику по политике, также определим множество пользователей, ролей, типов (рис.4)

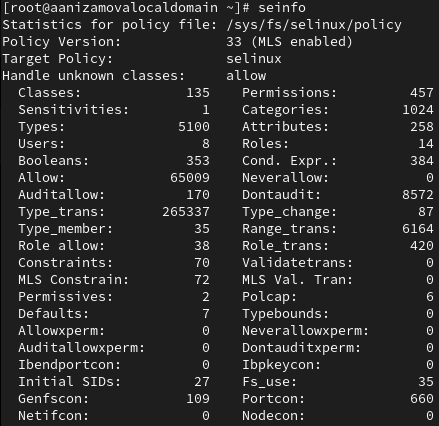


Рис. 4

1. Определим тип файлов и поддиректорий, находящихся в директории */var/www* (рис.5)

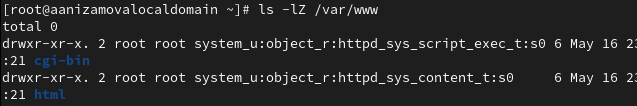
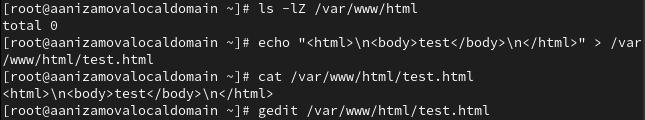
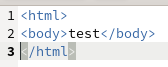


Рис. 5

1. Определим тип файлов, находящихся в директории */var/www/html* (рис.6)
2. Определим круг пользователей, которым разрешено создание файлов в директории */var/www/html* - только суперпользователь (рис.6)
3. Создадим от имени суперпользователя html-файл */var/www/html/test.html* (рис.6-7)

1. Проверим контекст созданного файла. (рис.8)

Рис. 8

Рис. 8

1. Обратимся к файлу через веб-сервер (рис.9)

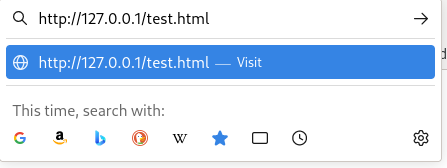


Рис. 9

1. Изучим справку man httpd\_selinux и выясним, какие контексты файлов определены для httpd. Выдало, что справки нет (рис.10)
2. Изменим контекст файла */var/www/html/test.html* с *httpd\_sys\_content\_t* на *samba\_share\_t*.  
   После этого проверим, что контекст поменялся (рис.10)

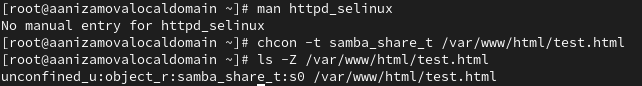


Рис. 10

1. Попробуем ещё раз получить доступ к файлу через веб-сервер, мы должны получить сообщение об ошибке (рис.11)

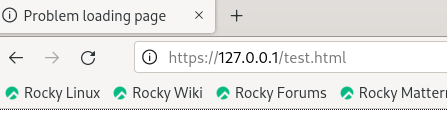


Рис. 11

1. Просмотрим log-файлы веб-сервера Apache. Также просмотрим системный лог-файл (рис.12)

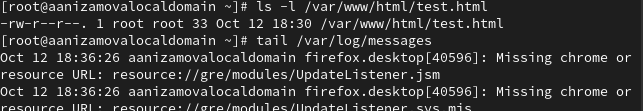


Рис. 12

1. Попробуем 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* заменим строчку *Listen 80* на *Listen 81* (рис.13)

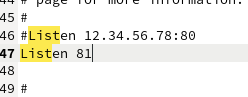


Рис. 13

1. Выполним перезапуск веб-сервера Apache. (рис.14)
2. Проанализируем лог-файлы. Просмотрим файлы */var/log/http/error\_log*, */var/log/http/access\_log* и */var/log/audit/audit.log* и выясним, в каких файлах появились записи. (рис.14)

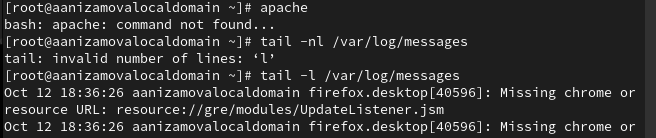


Рис. 14

1. Выполним заданную в методичке команду.  
   После этого проверим список портов. Убедимся, что порт 81 появился в списке (рис.15)
2. Попробуем запустить веб-сервер Apache ещё раз (рис.15)

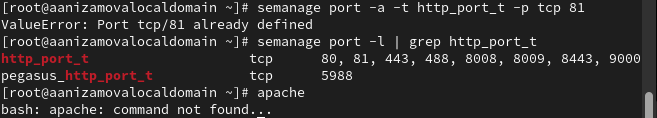


Рис. 15

1. Вернем контекст \*httpd\_sys\_cоntent\_\_t\* к файлу */var/www/html/ test.html* (рис.16)
2. Исправим обратно конфигурационный файл apache, вернув *Listen 80* (рис.16)

Рис. 16

Рис. 16

1. Удалим привязку *http\_port\_t* к 81 порту и проверим, что порт 81 удалён (рис.17)
2. Удалим файл */var/www/html/test.html* (рис.17)

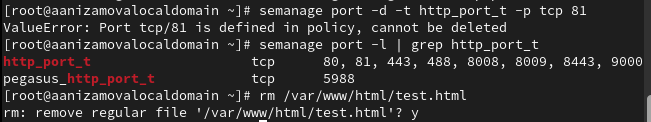


Рис. 17

# 3 Вывод

Мы развили навыки администрирования ОС Linux, а также получили первое практическое знакомство с технологией SELinux1.  
Проверили работу SELinx на практике совместно с веб-сервером Apache.