Отчёт по лабораторной работе №6

Дисциплина: Основы информационной безопасности

Барсегян Вардан Левонович НПИбд-01-22

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

1. Убеждаюсь, что SELinux работает в режиме enforcing политики targeted с помощью команд *getenforce* и *sestatus*. Запускаю веб-сервер командой *service httpd start* и проверяю его статус командой *service httpd status* (рис. 1)

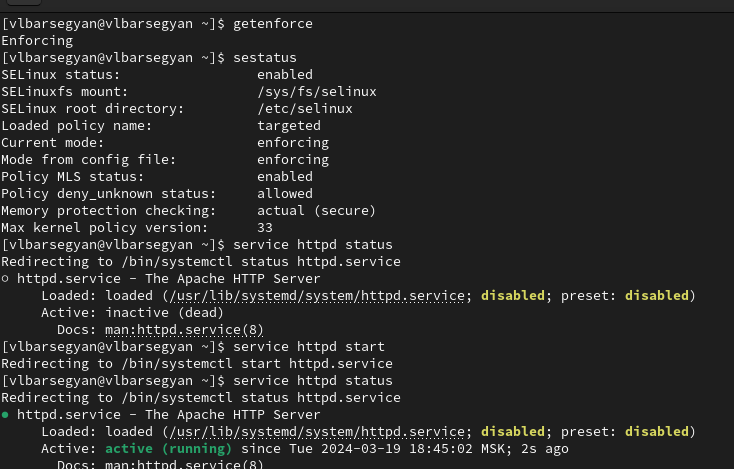


Рис. 1: Запуск и проверка веб-сервера

1. Определяю контекст безопасности веб-сервера с помощью команды *ps auxZ | grep httpd* (рис. 2)

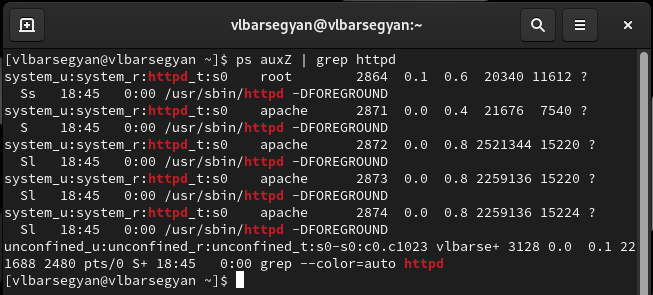


Рис. 2: Контекст безопасности веб-сервера

1. Просматриваю текущее состояние переключателей SELinux для Apache с помощью команды *sestatus -b | grep httpd* (рис. 3)

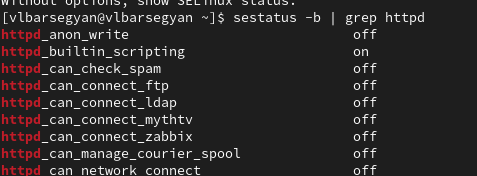


Рис. 3: Состояние переключателей SELinux

1. Смотрю статистику по политике с помощью команды *seinfo* (рис. 4)

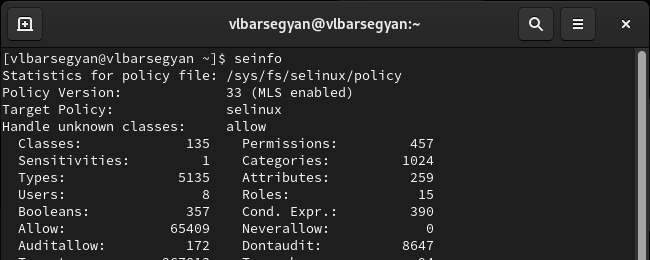


Рис. 4: Статистика по политике

1. Определяю тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды *ls -lZ /var/www*. Аналогично для директории /var/www/html (рис. 5)

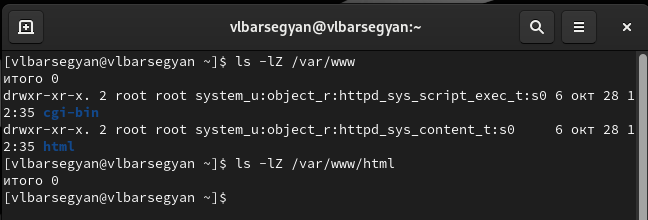


Рис. 5: Определение типа файлов и папок

1. Создаю файл /var/www/html/test.html и записываю следующий html-код (рис. 6)

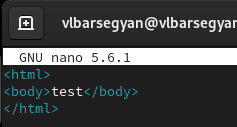


Рис. 6: test.html

1. Проверяю контекст созданного файла командой *ps auxZ | grep test.html* (рис. 7)

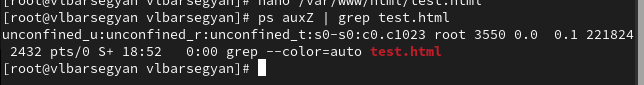


Рис. 7: Контекст файла

1. Проверяю в браузере, что файл успешно отображается (рис. 8)

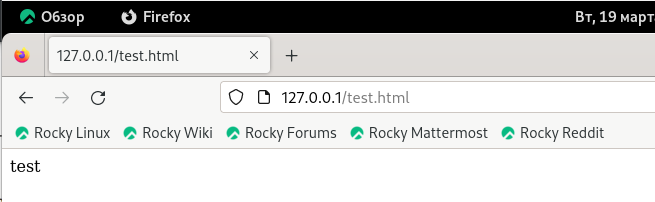


Рис. 8: Проверка в браузере

1. Изучаю справку man по командам httpd и selinux, также проверяю контекст файла командой *ls -Z /var/www/html/test.html* (рис. 9)

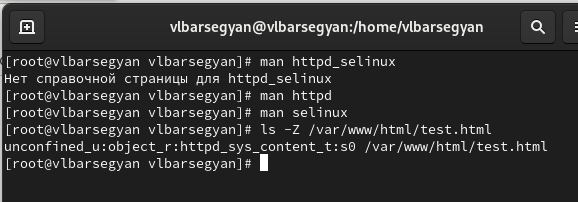


Рис. 9: Изучение man, проверка контекста

1. Изменяю контекст файла test.html командой *chcon -t samba\_share\_t /var/www/html/test.html*. После, проверяю его и открываю веб-страницу - нет доступа (рис. 10)

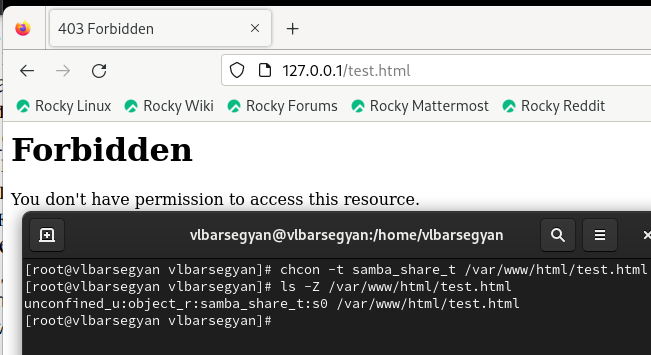


Рис. 10: Изменение контекста

1. Просматриваю системный лог-файл командой *tail /var/log/messages* (рис. 11)

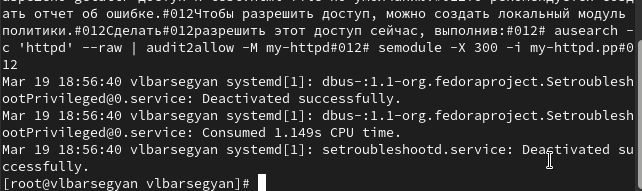


Рис. 11: Системный лог-файл

1. В файле /etc/httpd/conf/httpd.conf меняю порт на 81 (рис. 12)

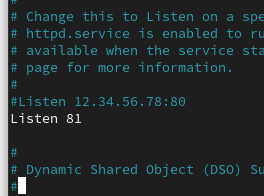


Рис. 12: Смена порта

1. Перезагружаю веб-сервер - получен сбой (рис. 13)

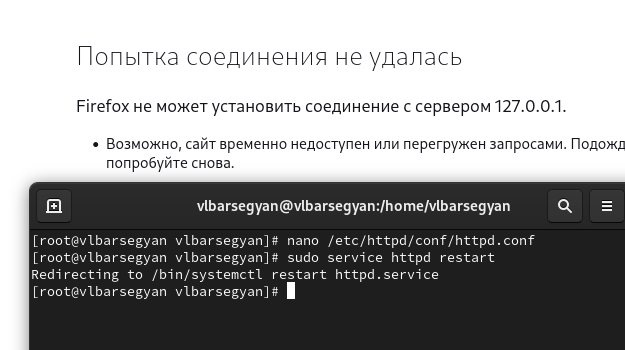


Рис. 13: Сбой веб-сервера

1. Анализирую лог-файлы командами *tail -nl /var/log/messages* и *cat /var/log/http/error\_log* (рис. 14)

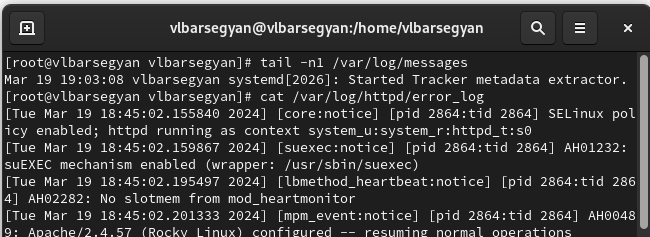


Рис. 14: Проверка лог-файлов

1. Также проверяю лог-файл */var/log/http/access\_log* (рис. 15)

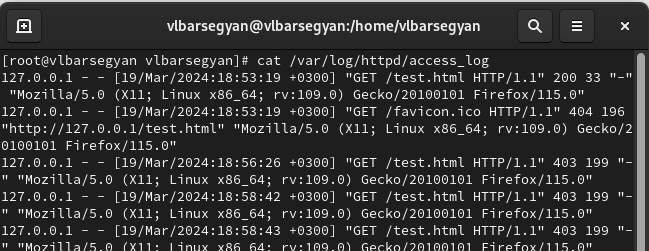


Рис. 15: Проверка лог-файлов

1. Также проверяю лог-файл */var/log/audit/audit.log*. (рис. 16)

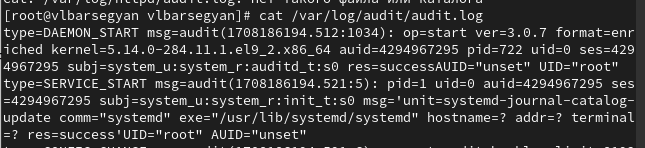


Рис. 16: Проверка лог-файлов

1. Выполняю команду *semanage port -a -t http\_port\_t -р tcp 81* и проверяю список портов командой *semanage port -l | grep http\_port\_t* - порт 81 появился в списке (рис. 17)

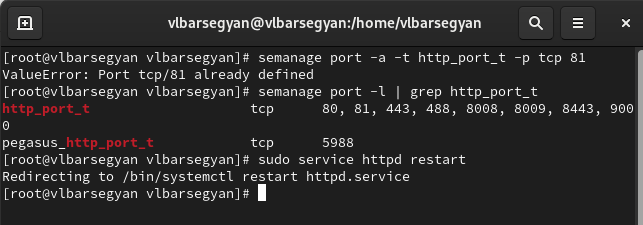


Рис. 17: Добавление порта 81 в список

1. Возвращаю контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html, введя *chcon -t httpd\_sys\_content\_t /var/www/html/test.html*. Перезапускаю веб-сервер командой *sudo service httpd restart* (рис. 18)

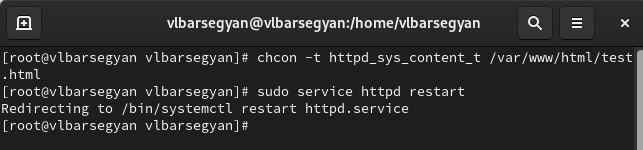


Рис. 18: Возвращение контекста и перезапуск веб-сервера

1. Возвращаю порт 80 в конфигурационном файле (рис. 19)

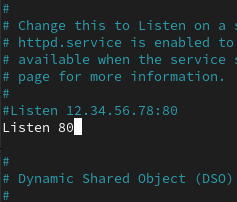


Рис. 19: Смена порта на 80

1. Удаляю привязку http\_port\_t к 81 порту командой *semanage port -d -t http\_port\_t -p tcp 81* и удаляю файл test.html командой *rm /var/www/html/test.html* (рис. 20)

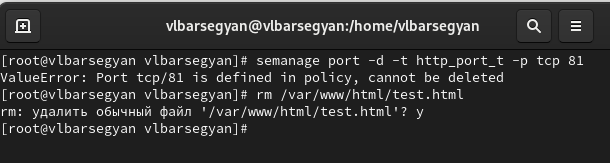


Рис. 20: Удаление привязки к 81 порту и удаление html-файла

# 3 Выводы

Я развил навыки администрирования ОС Linux, познакомился с технологией SELinux, поработал с веб-сервером Apache

# Список литературы