Отчёт по лабораторной работе №6

Дисциплина: Основы информационной безопасности

Барсегян Вардан Левонович НПИбд-01-22

Содержание

Список иллюстраций

Список таблиц

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. 2.1)

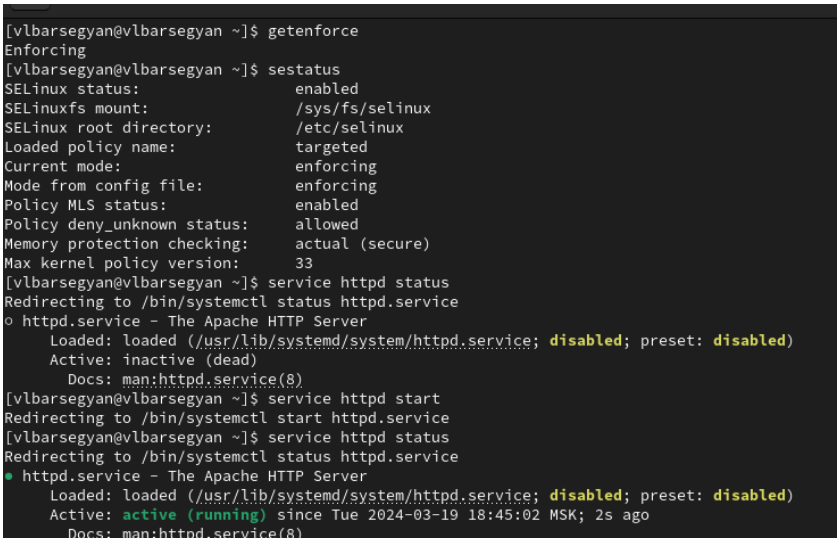

Рис. 2.1: Запуск и проверка веб-сервера

2. Определяю контекст безопасности веб-сервера с помощью команды *ps auxZ | grep httpd* (рис. 2.2)

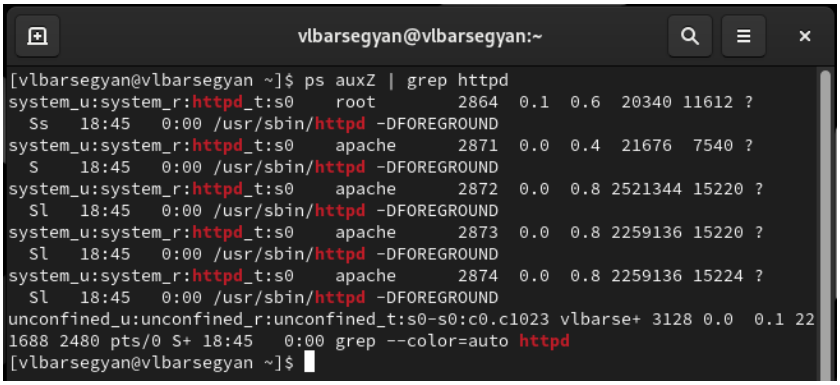

Рис. 2.2: Контекст безопасности веб-сервера

3. Просматриваю текущее состояние переключателей SELinux для Apache с помощью команды *sestatus -b | grep httpd* (рис. 2.3)

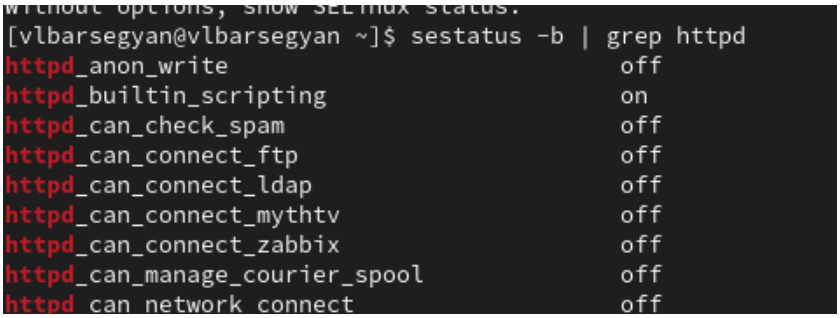

Рис. 2.3: Состояние переключателей SELinux

4. Смотрю статистику по политике с помощью команды *seinfo* (рис. 2.4)

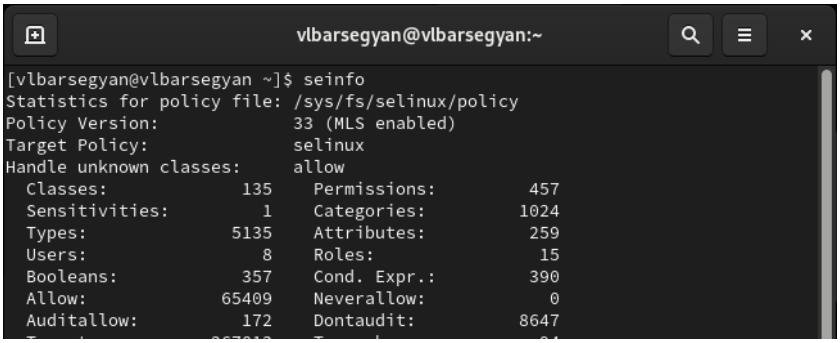

Рис. 2.4: Статистика по политике

5. Определяю тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды *ls -lZ /var/www*. Аналогично для директории /var/www/html (рис. 2.5)

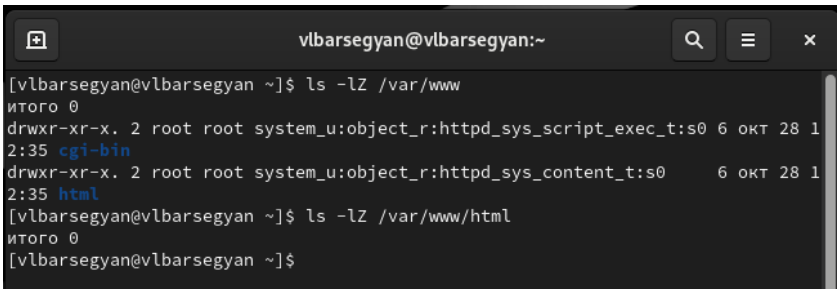

Рис. 2.5: Определение типа файлов и папок

6. Создаю файл /var/www/html/test.html и записываю следующий html-код (рис. 2.6)

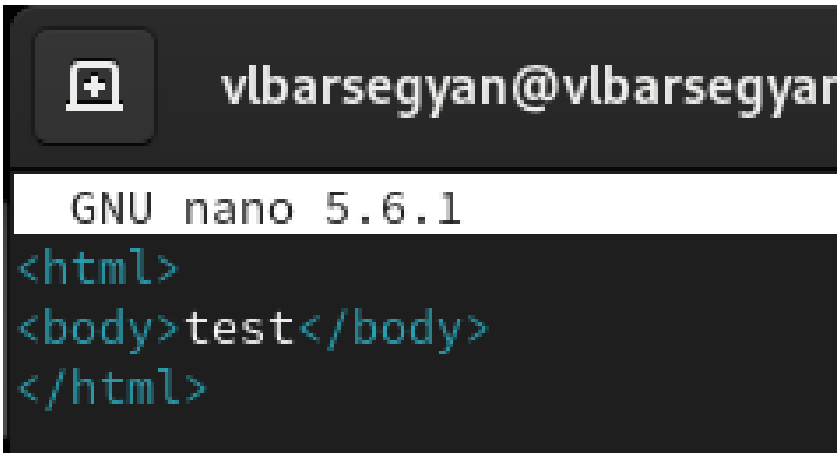

Рис. 2.6: test.html

7. Проверяю контекст созданного файла командой *ps auxZ | grep test.html* (рис. 2.7)

Рис. 2.7: Контекст файла

8. Проверяю в браузере, что файл успешно отображается (рис. 2.8)

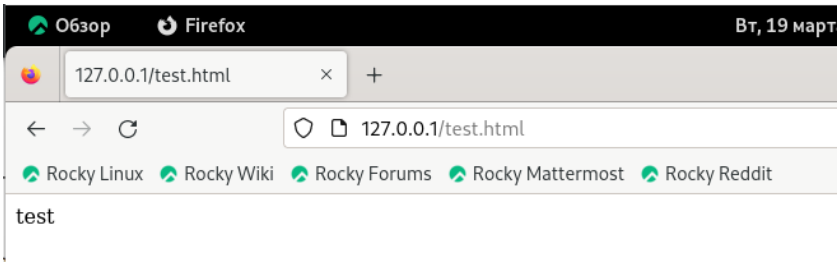

Рис. 2.8: Проверка в браузере

9. Изучаю справку man по командам httpd и selinux, также проверяю контекст файла командой *ls -Z /var/www/html/test.html* (рис. 2.9)

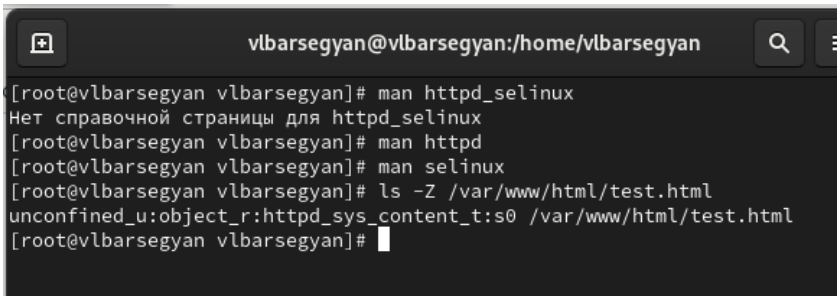

Рис. 2.9: Изучение man, проверка контекста

10. 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. 2.10)

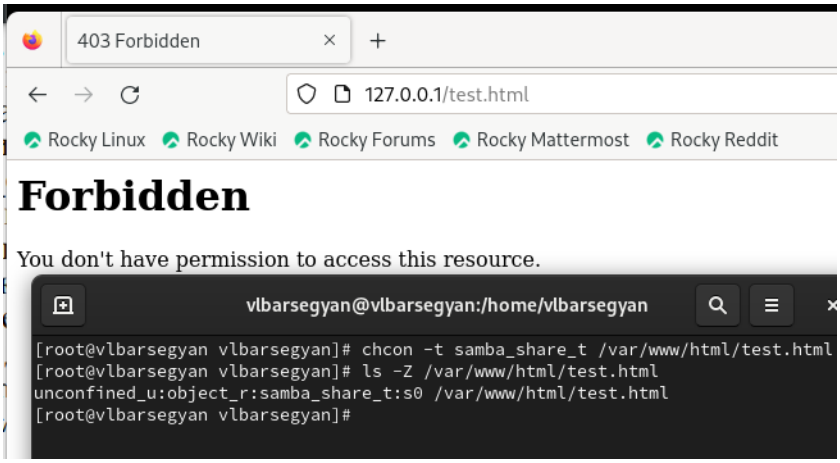

Рис. 2.10: Изменение контекста

11. Просматриваю системный лог-файл командой *tail /var/log/messages* (рис. 2.11)

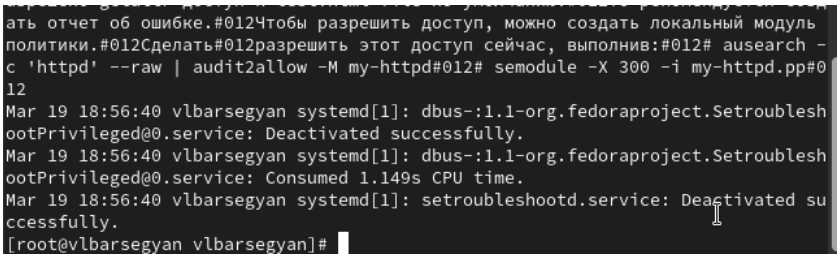

Рис. 2.11: Системный лог-файл

12. В файле /etc/httpd/conf/httpd.conf меняю порт на 81 (рис. 2.12)

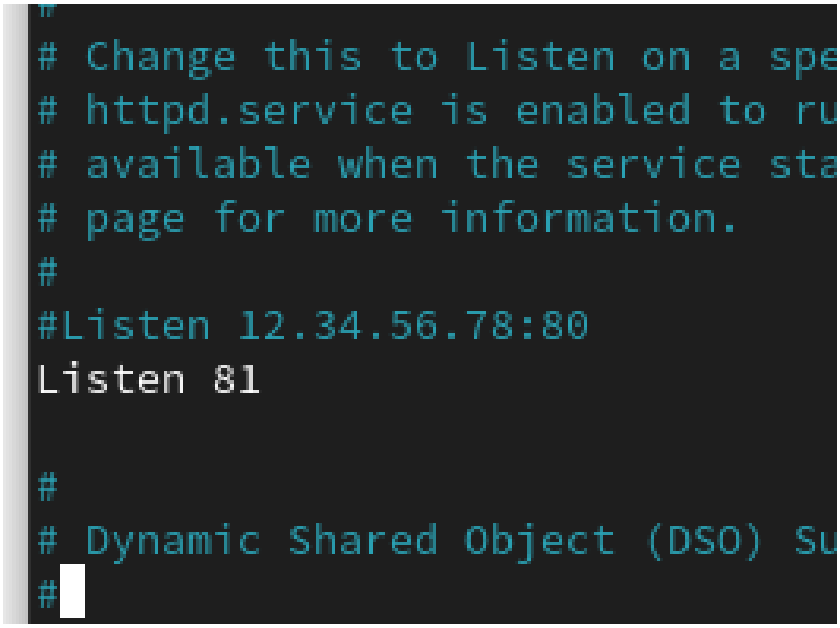

Рис. 2.12: Смена порта

13. Перезагружаю веб-сервер - получен сбой (рис. 2.13)

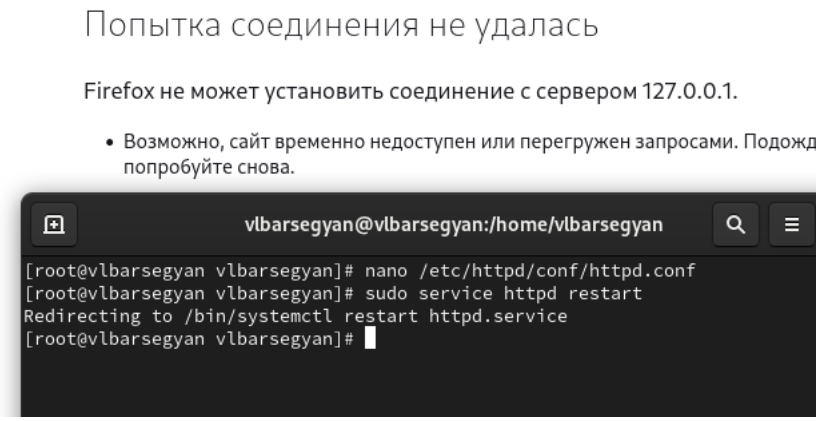

Рис. 2.13: Сбой веб-сервера

14. Анализирую лог-файлы командами *tail -nl /var/log/messages* и *cat /var/log/http/error_log* (рис. 2.14)

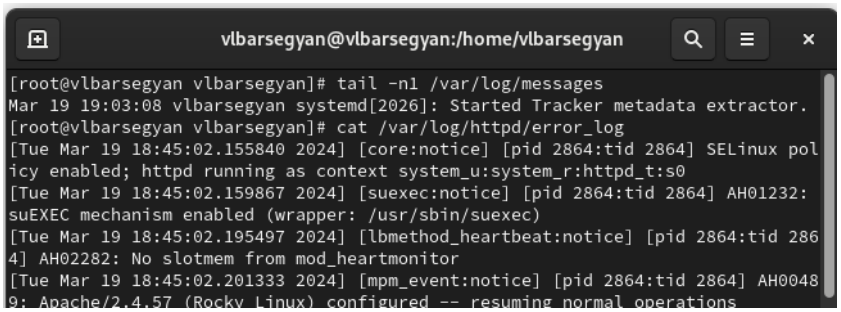

Рис. 2.14: Проверка лог-файлов

15. Также проверяю лог-файл */var/log/http/access_log* (рис. 2.15)

Рис. 2.15: Проверка лог-файлов

16. Также проверяю лог-файл */var/log/audit/audit.log*. (рис. 2.16)

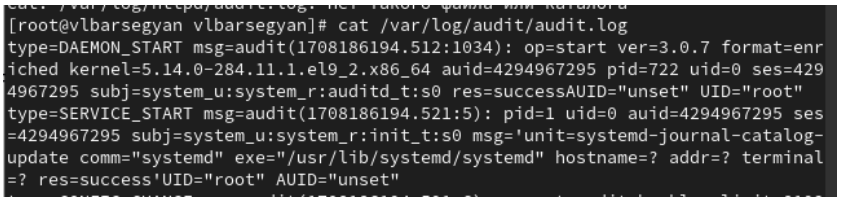

Рис. 2.16: Проверка лог-файлов

17. Выполняю команду *semanage port -a -t http_port_t -p tcp 81* и проверяю список портов командой *semanage port -l | grep http_port_t* - порт 81 появился в списке (рис. 2.17)

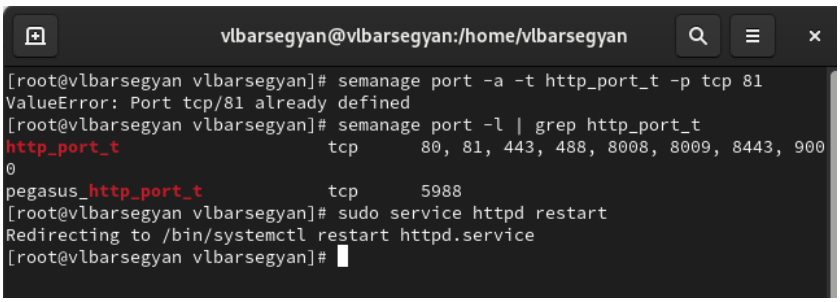

Рис. 2.17: Добавление порта 81 в список

18. Возвращаю контекст httpd_sys_content__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. 2.18)

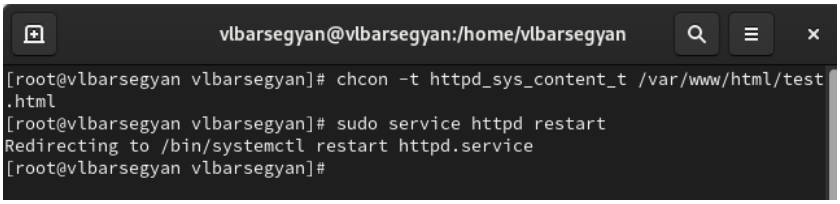

Рис. 2.18: Возвращение контекста и перезапуск веб-сервера

19. Возвращаю порт 80 в конфигурационном файле (рис. 2.19)

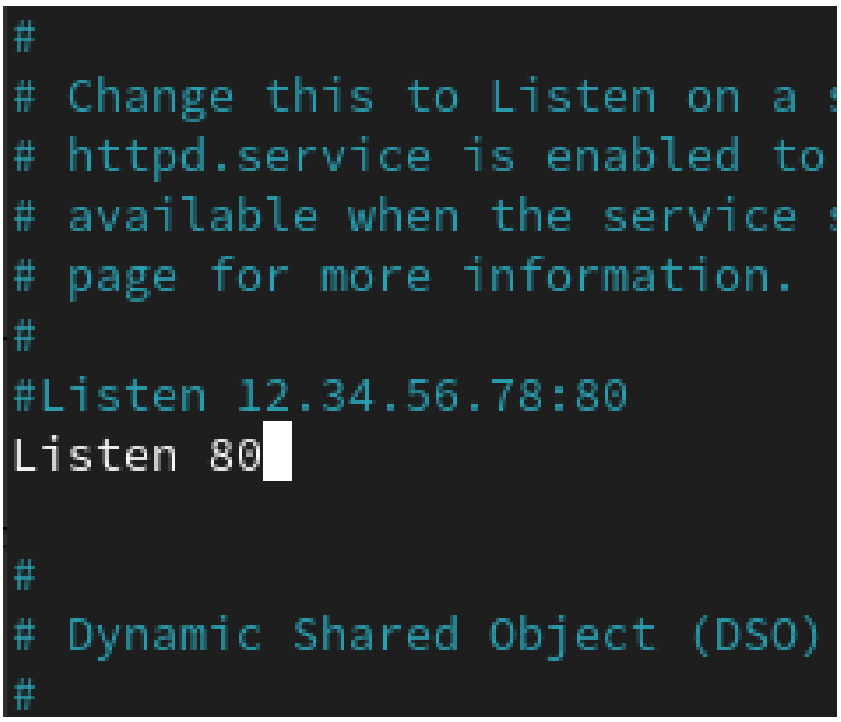

Рис. 2.19: Смена порта на 80

20. 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. 2.20)

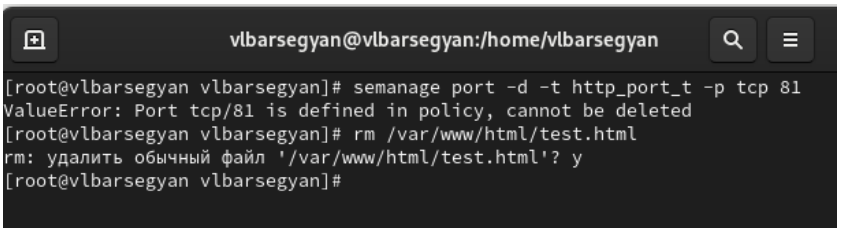

Рис. 2.20: Удаление привязки к 81 порту и удаление html-файла

3 Выводы

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

Список литературы