Лабораторная работа №6

Мандатное разграничение прав в Linux

Кувшинова К.О. группа НФИ-02-19

Содержание

List of Figures

1 Цель работы

Целью данной лабораторной работы является развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

2 Подготовка лабораторного стенда и методические рекомендации

1. Установили веб-сервер Apache командой **yum install httpd**. (fig. 2.1)

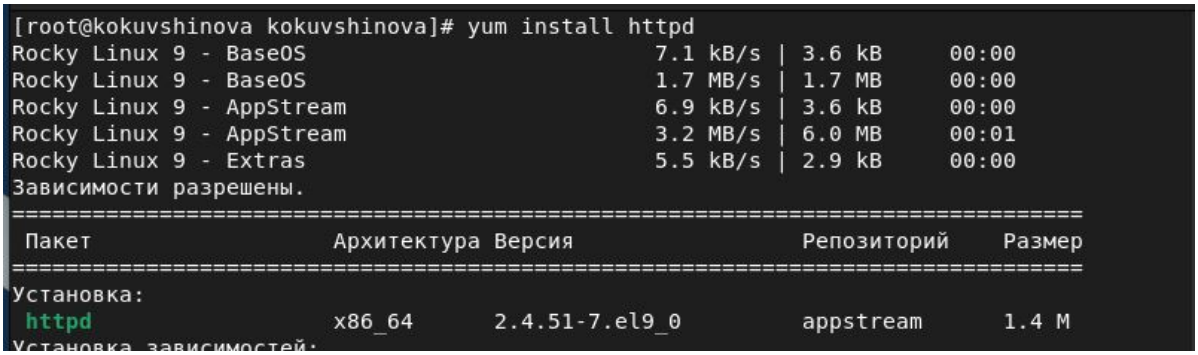

Figure 2.1: Установка веб-сервера Apache

2. В конфигурационном файле /etc/httpd/httpd.conf задали параметр ServerName. (fig. 2.2)

Figure 2.2: Установка параметра ServerName

3. Отключаем пакетный фильтр с помощью команд: (fig. 2.3)

iptables -F

iptables -P INPUT ACCEPT

iptables -P OUTPUT ACCEPT

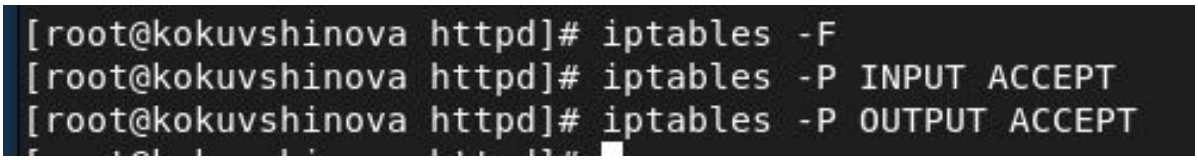

Figure 2.3: Отключение пакетного фильтра

3 Выполнение лабораторной работы

1. Входим в систему с полученными учётными данными. Проверили, что SELinux работает в режиме enforcing политики targeted с помощью команд **getenforce** и **sestatus**. (fig. 3.1)

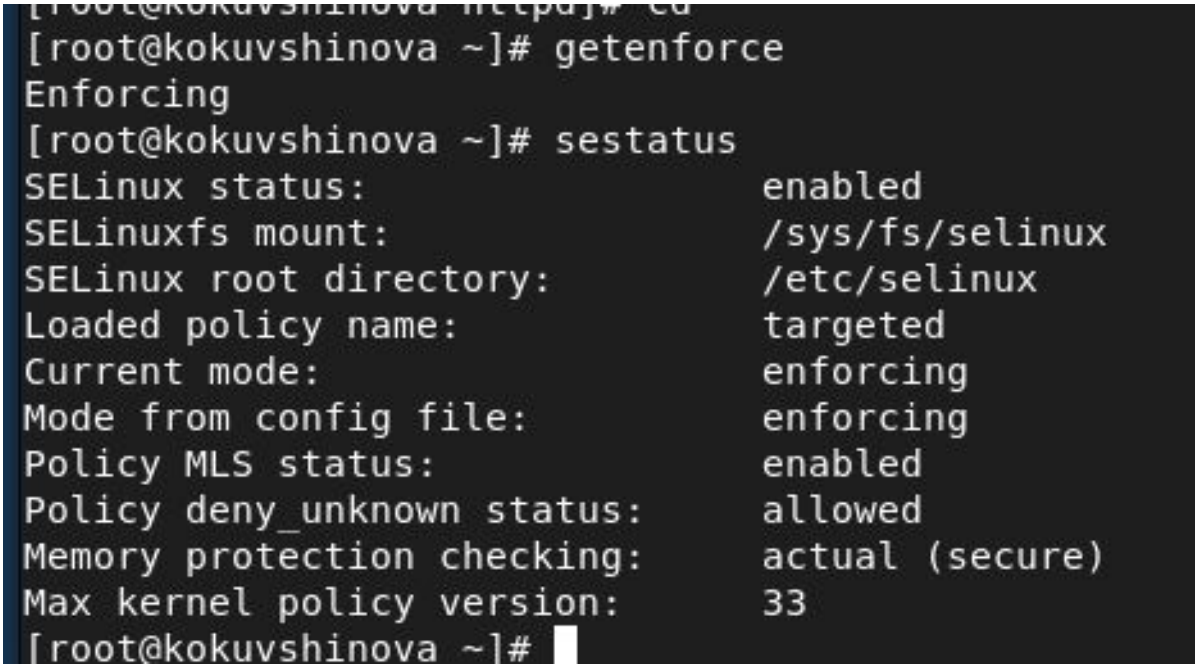

Figure 3.1: Выполнение команд getenforce и sestatus

2. Запустили веб-сервер и обратились к нему с помощью команд (fig. 3.2): service httpd start service httpd status

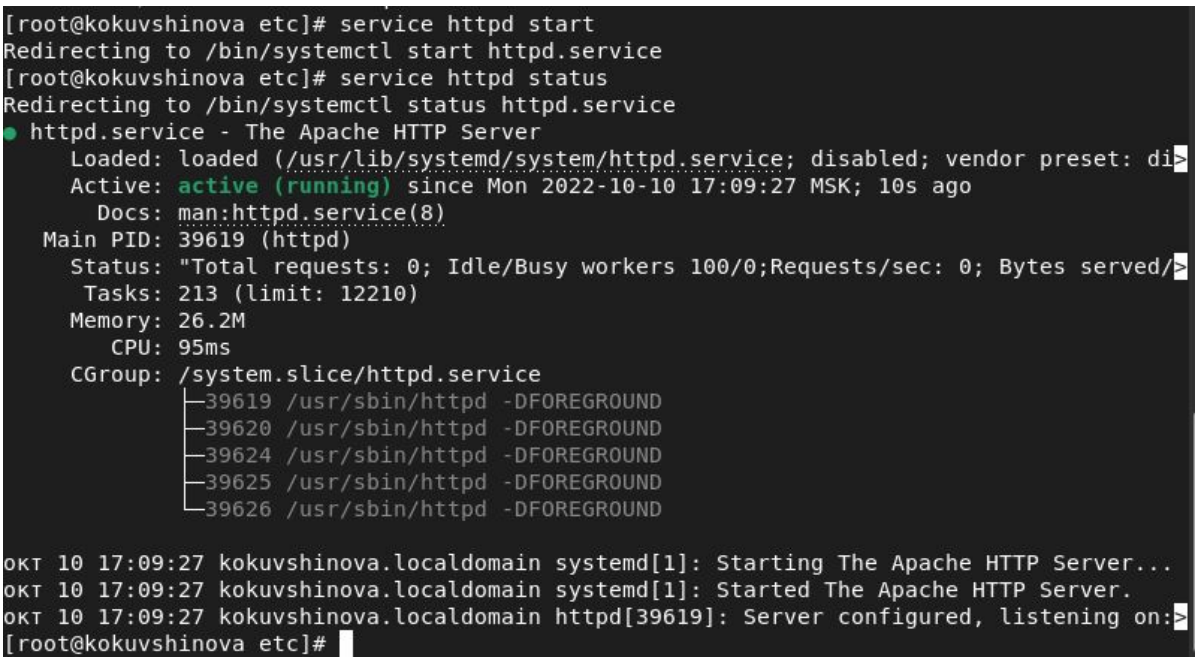

Figure 3.2: Выполнение команд service httpd start и status

3. Найшли веб-сервер Apache в списке процессов с помощью команды **ps auxZ | grep httpd**. Контекст безопасности - unconfined_u:unconfined_r:unconfined_t. (fig. 3.3)

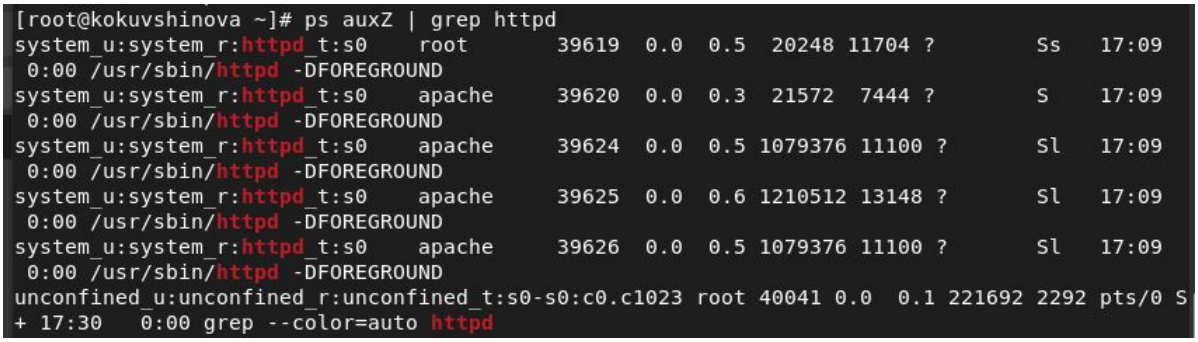

Figure 3.3: Выполнение команды ps auxZ | grep httpd

4. Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды **sestatus -b | grep httpd**. (fig. 3.4)

Figure 3.4: Выполнение команды sestatus -b | grep httpd

5. Посмотрели статистику по политике с помощью команды **seinfo**. Определили, что множество пользователей = 8; ролей = 14; типов = 5002. (fig. 3.5)

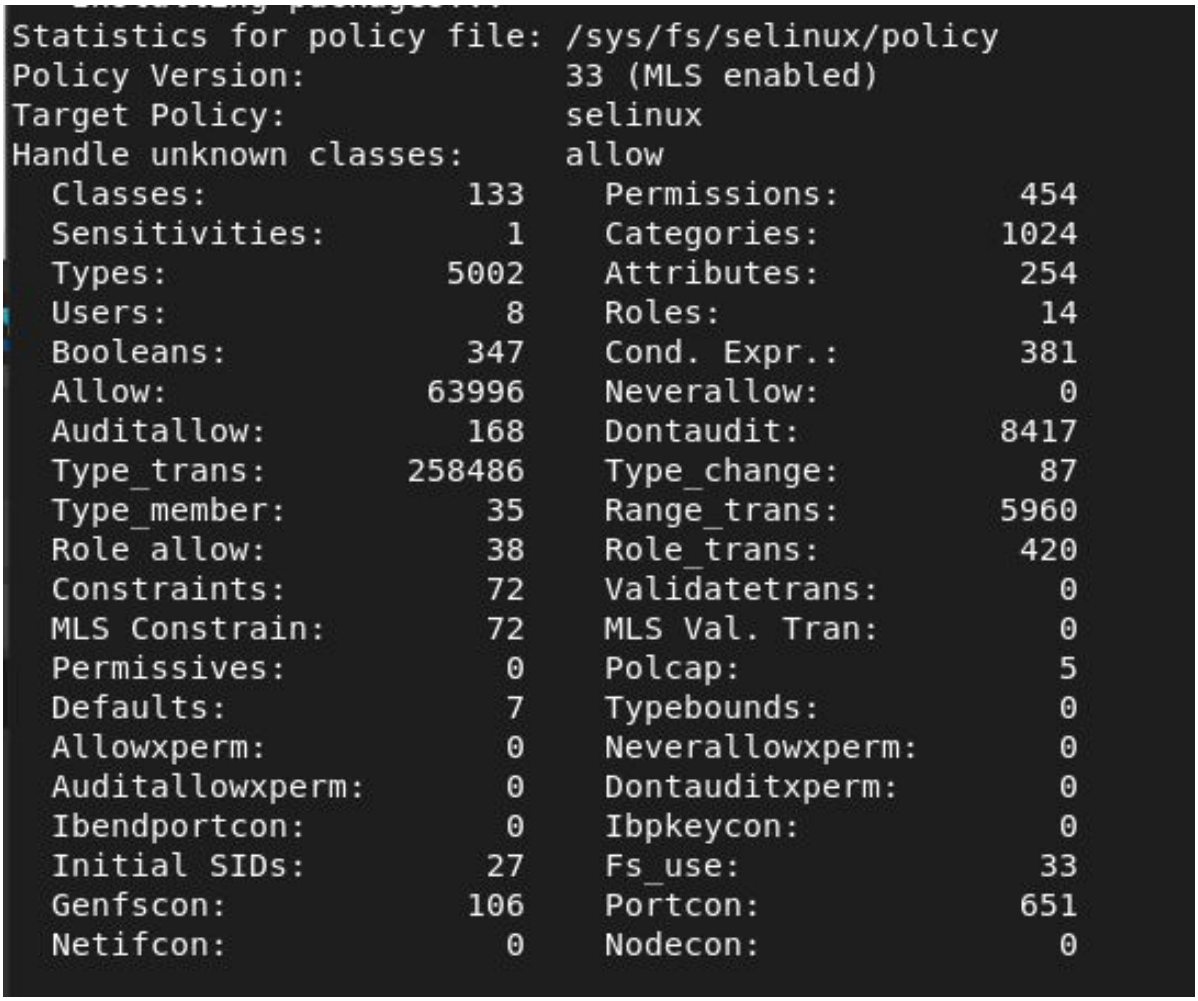

Figure 3.5: Статистика по политике

6. Определили тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды **ls -lZ /var/www**. (fig. 3.6)

Figure 3.6: Выполнение команды ls -lZ /var/www

7. Необходимо было определить тип файлов, находящихся в директории /var/www/html, с помощью команды **ls -lZ /var/www/html**. Но в данной директории файлов не обнаружилось. (fig. 3.7)

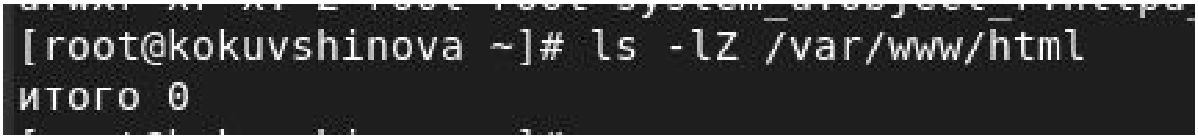

Figure 3.7: Выполнение команды ls -lZ /var/www/html

8. Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html - только uesr. (fig. 3.8)

Figure 3.8: Выполнение команды ls -lZ /var/www

9. Создали от имени суперпользователя html-файл /var/www/html/test.html следующего содержания: (fig. 3.9)

Figure 3.9: Содержимое файла test.html

10. Проверили контекст созданного файла - httpd_sys_content_t. (fig. 3.10)

Figure 3.10: Контекст файла test.html

11. Обратитились к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html и убедились, что файл был успешно отображён. (fig. 3.11)

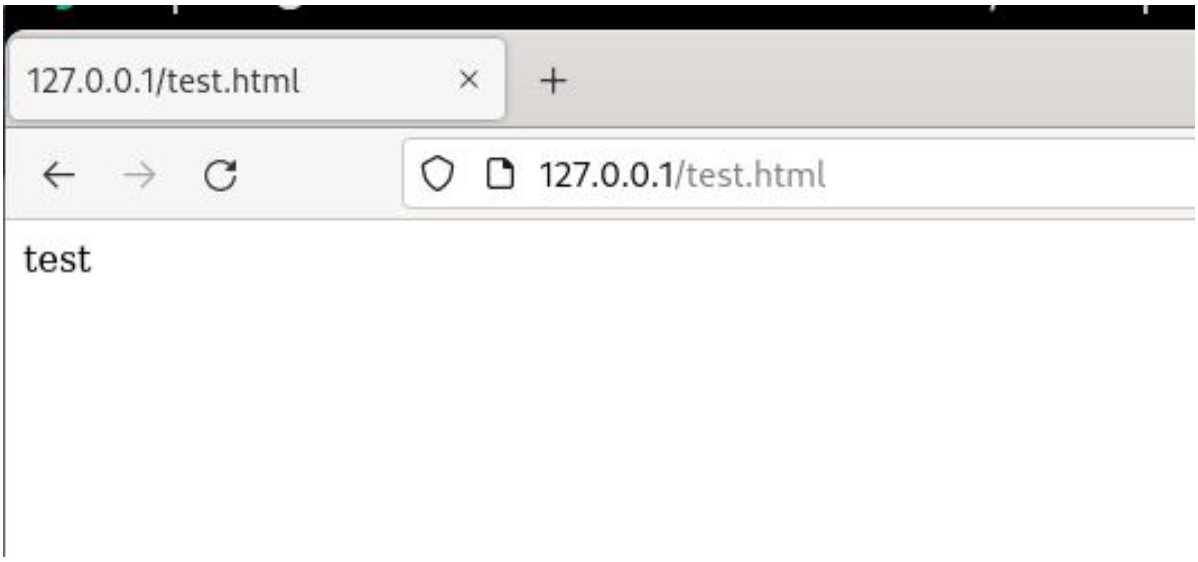

Figure 3.11: Обращение к файлу test.html через веб-сервер

12. Изучили справку man httpd_selinux. Тип файла test.html - контекст созданного файла - httpd_sys_content_t. (fig. 3.12)

Figure 3.12: Контекст файла test.html

13. Изменили контекст файла /var/www/html/test.html с httpd_sys_content_t на samba_share_t: chcon -t samba_share_t /var/www/html/test.html ls -Z /var/www/html/test.html И проверили, что контекст поменялся. (fig. 3.13)

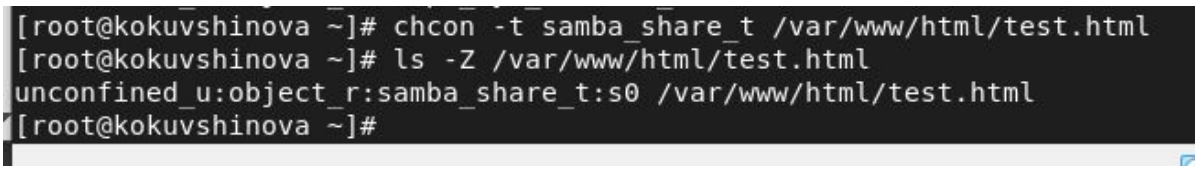

Figure 3.13: Изменение контекста файла /var/www/html/test.html

14. Пробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. В результате получили ошибку. (fig. 3.14)

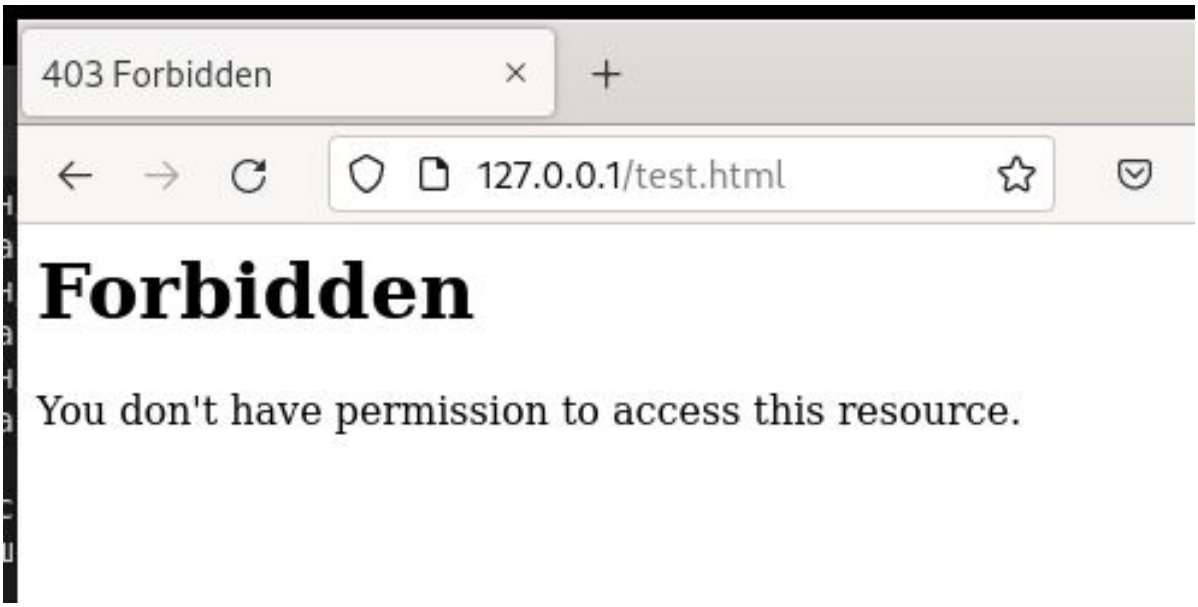

Figure 3.14: Обращение к файлу test.html через веб-сервер после изменения контекста

15. Проанализируем ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? ls -l /var/www/html/test.html Просмотрим log-файлы веб-сервера Apache и системный лог-файл: tail /var/log/messages В системе оказались запущенны процессы **setroubleshootd** и **audtd**. (fig. 3.15)

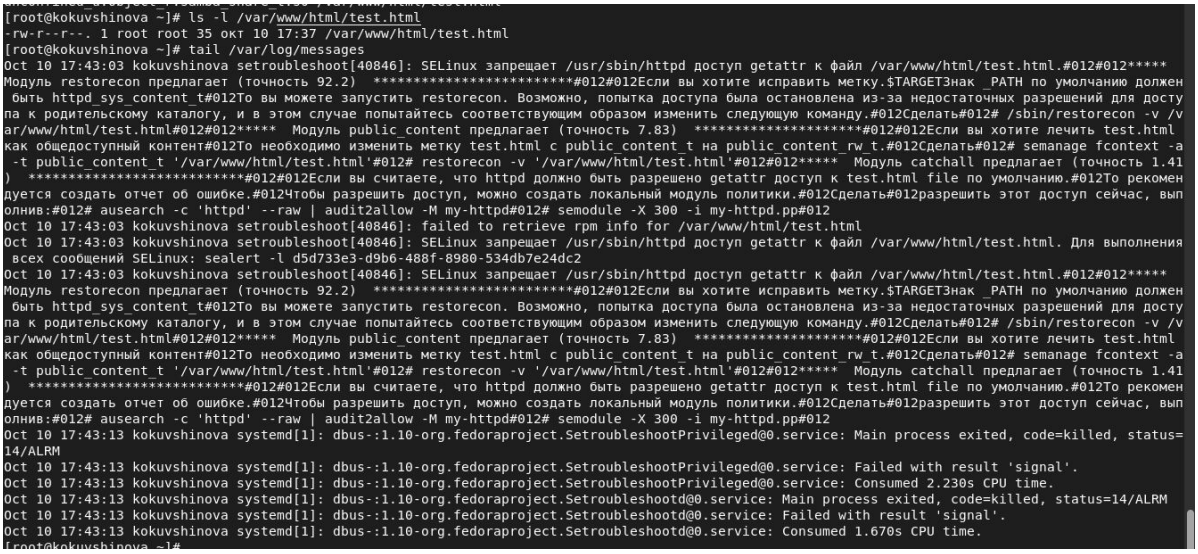

Figure 3.15: Вывод команд ls -l /var/www/html/test.html и tail /var/log/messages

16. Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле /etc/httpd/httpd.conf находим строчку Listen 80 и заменяем её на Listen 81. (fig. 3.16)

Figure 3.16: Запуск веб-сервера Apache на прослушивание TCP-порта 81

17. Выполним перезапуск веб-сервера Apache. Произошёл сбой? Нет.
18. Проанализируем лог-файлы: tail -nl /var/log/messages Просмотрим файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log. (fig. 3.17)

Figure 3.17: Перезапуск веб-сервера Apache

19. Выполним команду **semanage port -a -t http_port_t -p tcp 81**. Вылетает ValueError в связи с тем, что порт уже определен. После этого проверим список портов командой **semanage port -l | grep http_port_t** и убедились, что порт 81 появился в списке. (fig. 3.18)

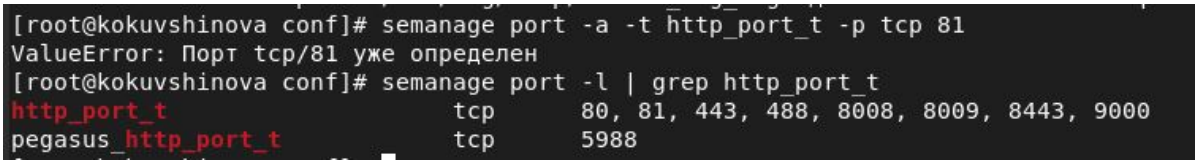

Figure 3.18: Проверка установления 81 порта tcp

20. Попробуем запустить веб-сервер Apache ещё раз. (fig. 3.19)

Figure 3.19: Перезапуск веб-сервера Apache

21. Вернули контекст httpd_sys_content__t к файлу /var/www/html/test.html: **chcon -t httpd_sys_content_t /var/www/html/test.html** (fig. 3.20)

Figure 3.20: Возвращение контекста httpd_sys_content__t к файлу test.html

После этого пробуем получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. В результате увидели содержимое файла — слово «test». (fig. 3.21)

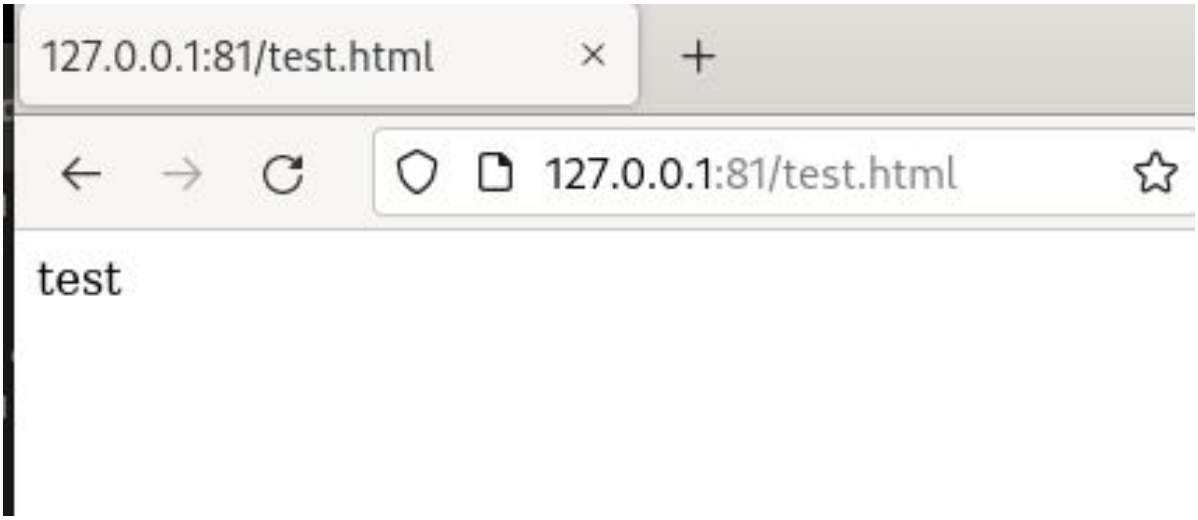

Figure 3.21: Обращение к файлу test.html через веб-сервер

22. Исправим обратно конфигурационный файл apache, вернув Listen 80. (fig. 3.22)

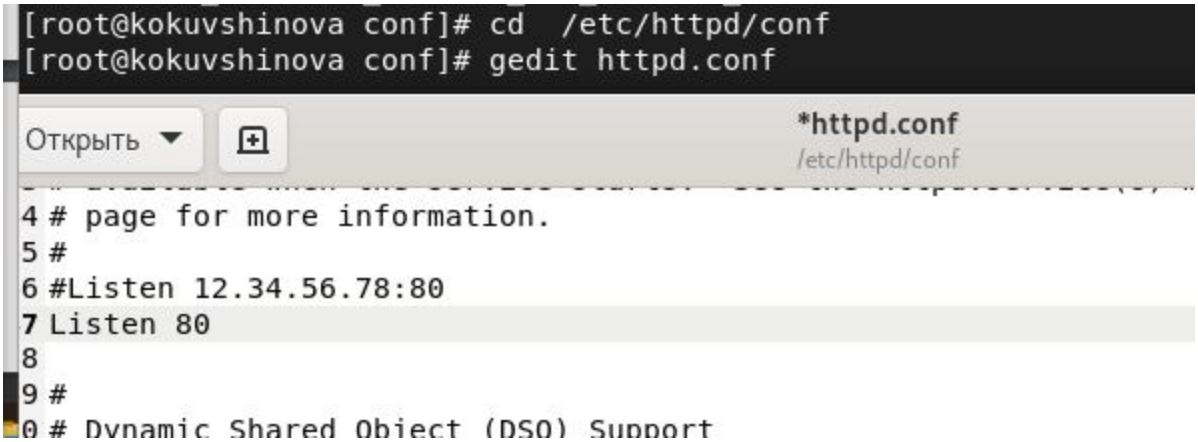

Figure 3.22: Исправление конфигурационного файла apache

23. Удалим привязку http_port_t к 81 порту: **semanage port -d -t http_port_t -p tcp 81** и проверим, что порт 81 удалён. Данная команда не была выполнена. (fig. 3.23)

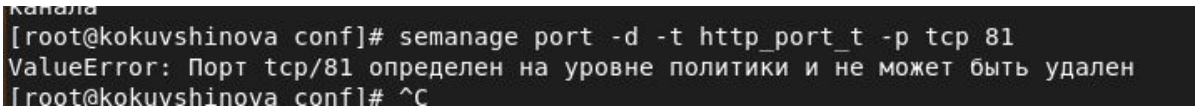

Figure 3.23: Удаление привязки http_port_t к 81 порту

24. Удалим файл /var/www/html/test.html: **rm /var/www/html/test.html**. (fig. 3.24)

Figure 3.24: Удаление файла test.html

4 Вывод

В ходе выполнения лабораторной работы мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.

5 Библиография

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Мандатное разграничение прав в Linux [Текст] / Кулябов Д. С., Королькова А. В., Геворкян М. Н. - Москва: - 5 с. [^1]: Мандатное разграничение прав в Linux.
2. Справочник 70 основных команд Linux: полное описание с примерами (https://eternalhost.net/blog/sozdanie-saytov/osnovnye-komandy-linux)