Отчет по лабораторной работе №6

по дисциплине: Информационная безопасность

Ким Михаил Алексеевич

Содержание

# 1 Цель работы

Развитие навыков администрирования ОС Linux. Получение первого практического знакомства с технологией SELinux. Проверка работы SELinx на практике совместно с веб-сервером Apache.

# 2 Задание

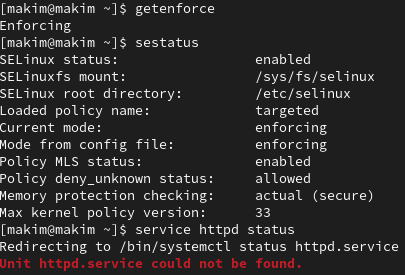
1. Произвести эксперименты с дополнительными атрибутами прав доступа.

# 3 Теоретическое введение

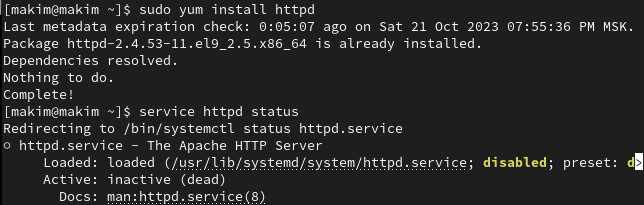
* Терминал (или «Bash», сокращение от «Bourne-Again shell») — это программа, которая используется для взаимодействия с командной оболочкой. Терминал применяется для выполнения административных задач, например: установку пакетов, действия с файлами и управление пользователями [1].
* Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами [2].
* В UNIX-системах, кроме стандартных прав доступа, существуют также дополнительные или специальные атрибуты файлов, которые поддерживает файловая система [3].
* SELinux (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра [4].
* Apache («Апачи», Apache HTTP Server) — это открытое кросс-платформенное программное обеспечение для размещения и поддержки веб-сервера [5].

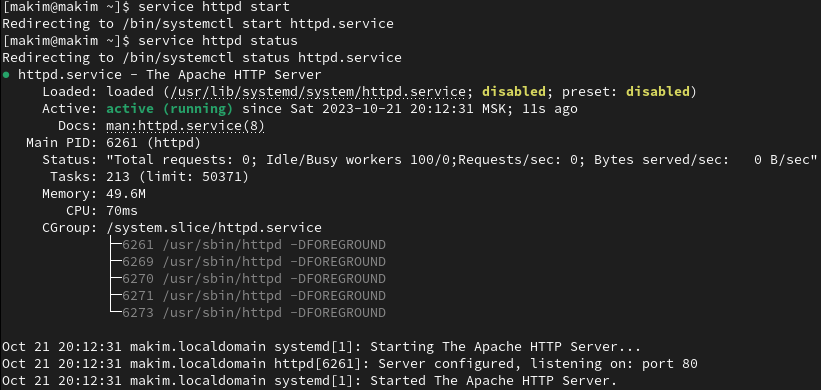
# 4 Выполнение лабораторной работы

1. Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus. (рис. [1](#fig:01)).

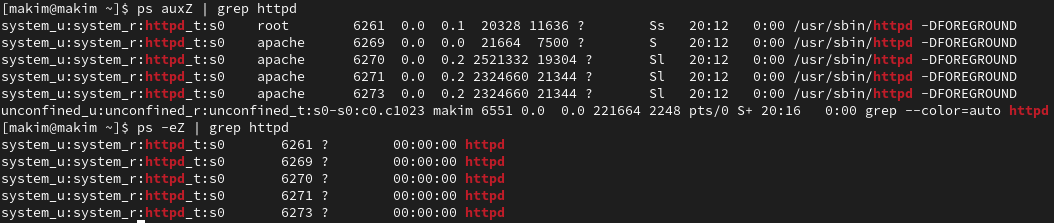
* 
* Figure 1: Проверка getenforce и sestatus

1. Обратимся с помощью браузера к веб-серверу, запущенному на компьютере, и убедимся, что последний работает: service httpd status. Предварительно установим пакет: sudo yum install httpd. Если не работает, запустим его так же, но с параметром start. (рис. [2](#fig:02), [3](#fig:03)).

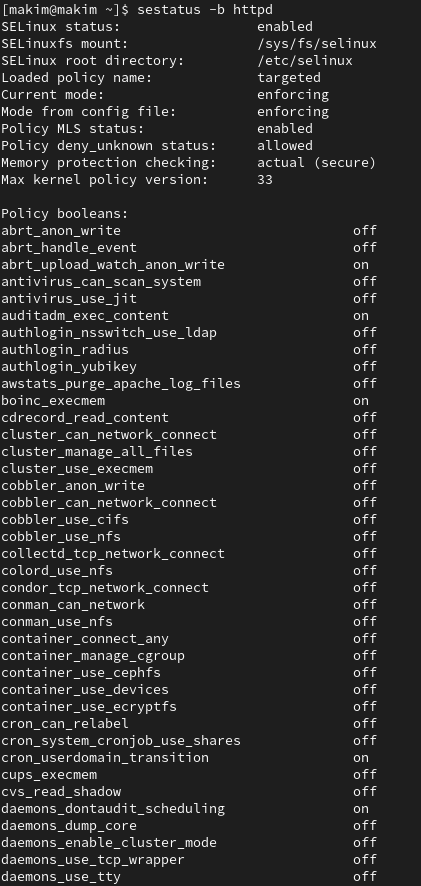
* 
* Figure 2: Установка и проверка статуса httpd

* 
* Figure 3: Запуск httpd

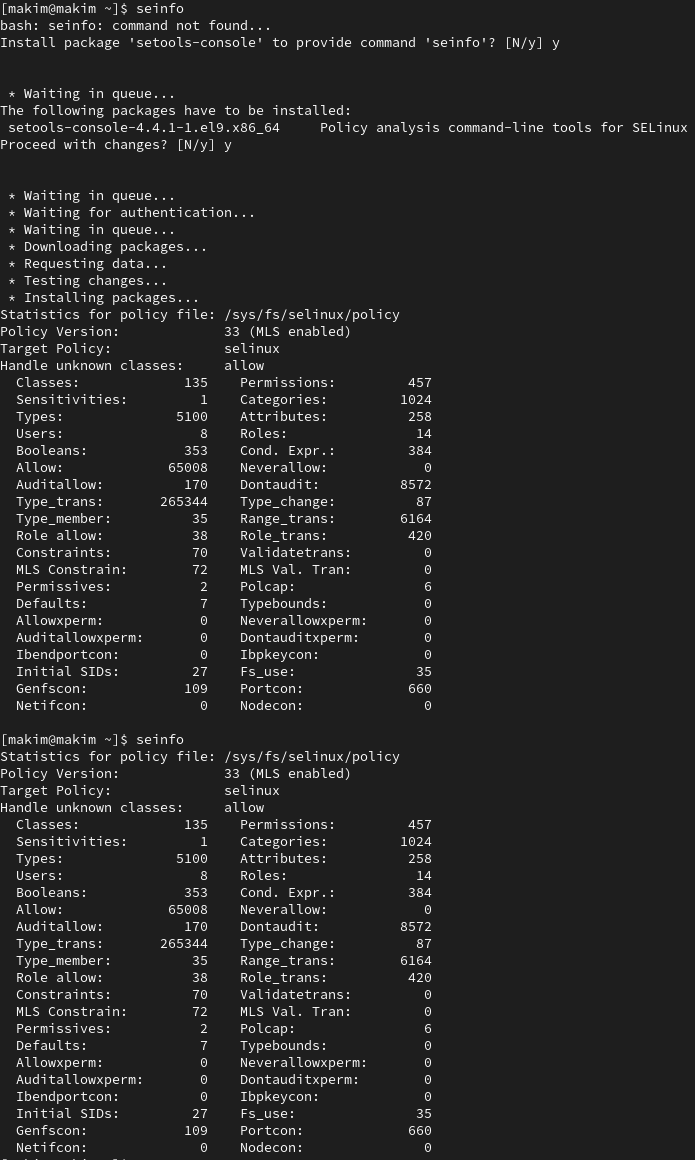
1. Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности и занесем эту информацию в отчёт. Например, можно использовать команды: ps auxZ | grep httpd, ps -eZ | grep httpd (рис. [4](#fig:04)).

* 
* Figure 4: Контекст безопасности httpd

1. Посмотрим текущее состояние переключателей SELinux для Apache с помощью команды sestatus -bigrep httpd (рис. [5](#fig:05)).

* 
* Figure 5: Текущее состояние переключателей SELinux для Apache

1. Посмотрим статистику по политике с помощью команды seinfo (предварительно установив необходимый пакет), также определим множество пользователей, ролей, типов. (рис. [6](#fig:06)).

* 
* Figure 6: Статистика по политике

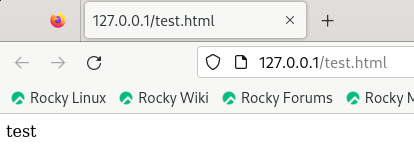
1. Определим тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www. Определим тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html: ll /var/www/html. Создадим от имени суперпользователя html-файл /var/www/html/test.html следующего содержания (рис. [7](#fig:07)): html <html> <body>test</body> </html>

* 
* Figure 7: Определение параметров и создание простого html-файла

1. Проверим контекст созданного файла: ls -Z /var/www/html.(рис. [8](#fig:08)).

* Figure 8: Контекст созданного файла
* Figure 8: Контекст созданного файла

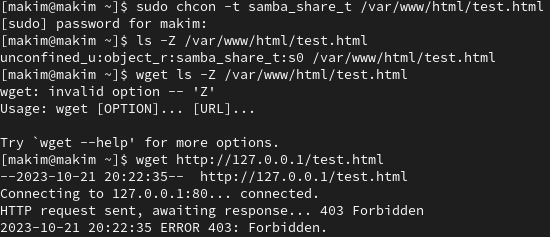
1. Обратимся к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедимся, что файл был успешно отображён. (рис. [9](#fig:09)).

* 
* Figure 9: Отображение файла test.html

1. Проверим контекст файла командой: ls -Z /var/www/html/test.html (рис. [10](#fig:10)).

* Figure 10: Проверка контекста файла test.html
* Figure 10: Проверка контекста файла test.html

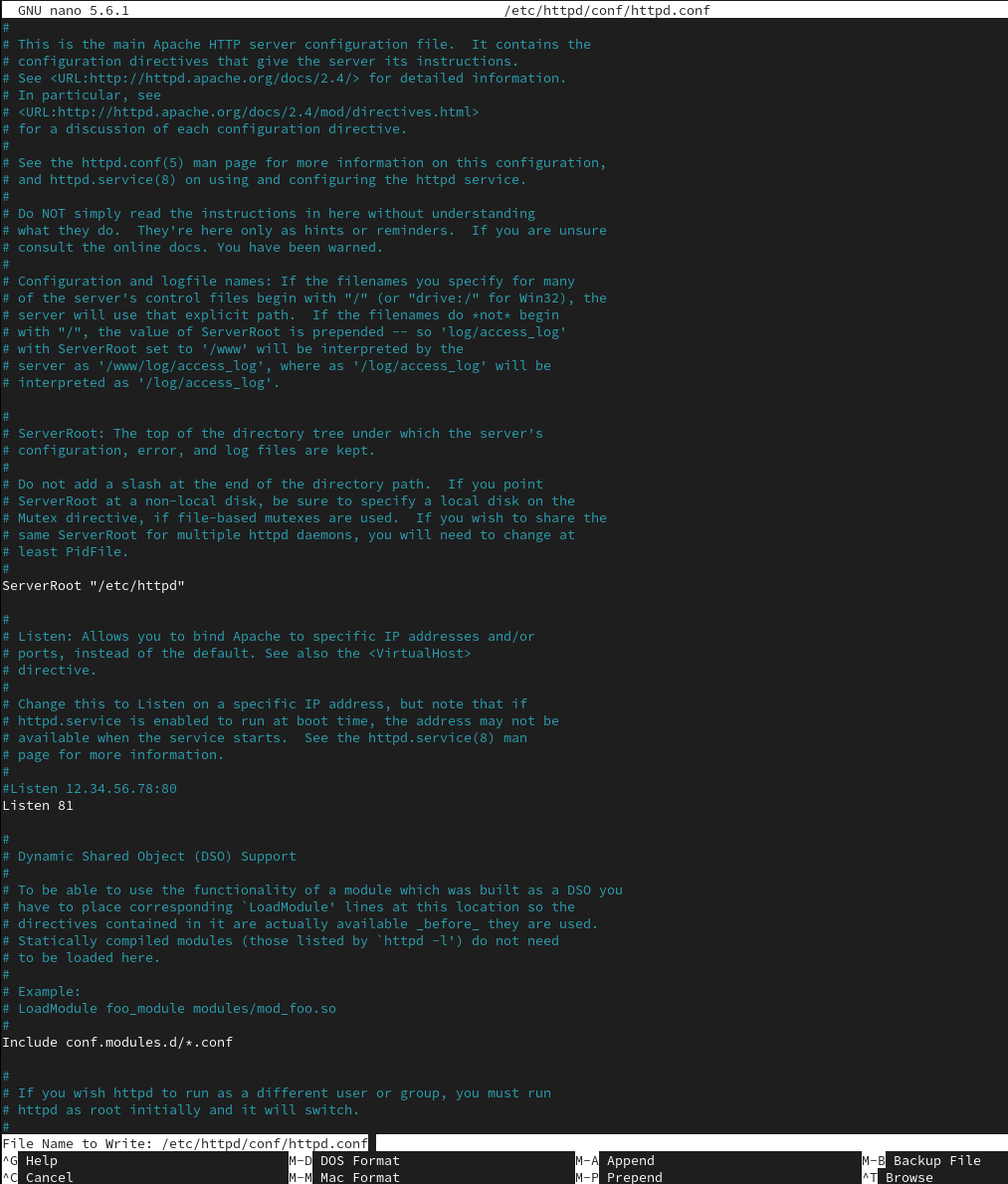
1. Изменим контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba\_share\_t: chcon -t samba\_share\_t /var/www/html/test.html, ls -Z /var/www/html/test.html. После этого проверим, что контекст поменялся. При попытку получить доступ к файлу получаем сообщение об ошибке (рис. [11](#fig:11)).

* 
* Figure 11: Изменение контекста файла test.html. Попытка получения доступа

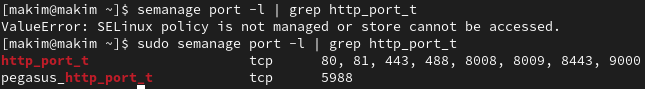
1. Просмотрим log-файлы (рис. [12](#fig:12)).

* 
* Figure 12: Log-файлы

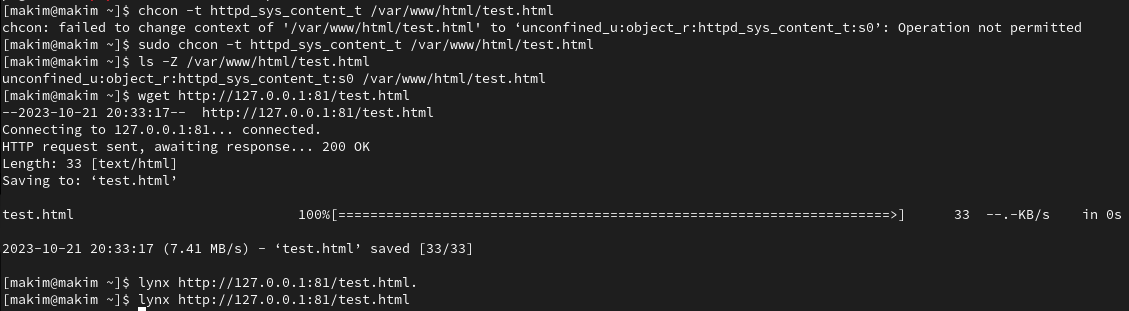
1. Попробуем запустить веб-сервер Apache на прослушивание ТСР-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдем строчку Listen 80 и заменим её на Listen 81 (рис. [13](#fig:13)).

* 
* Figure 13: Запуск веб-сервера Apacht на TCP-порт 81

1. Запустить веб-сервер удалось, т.к. TCP-порт 81 уже находится в списке прослушиваемых портов (рис. [14](#fig:14)).

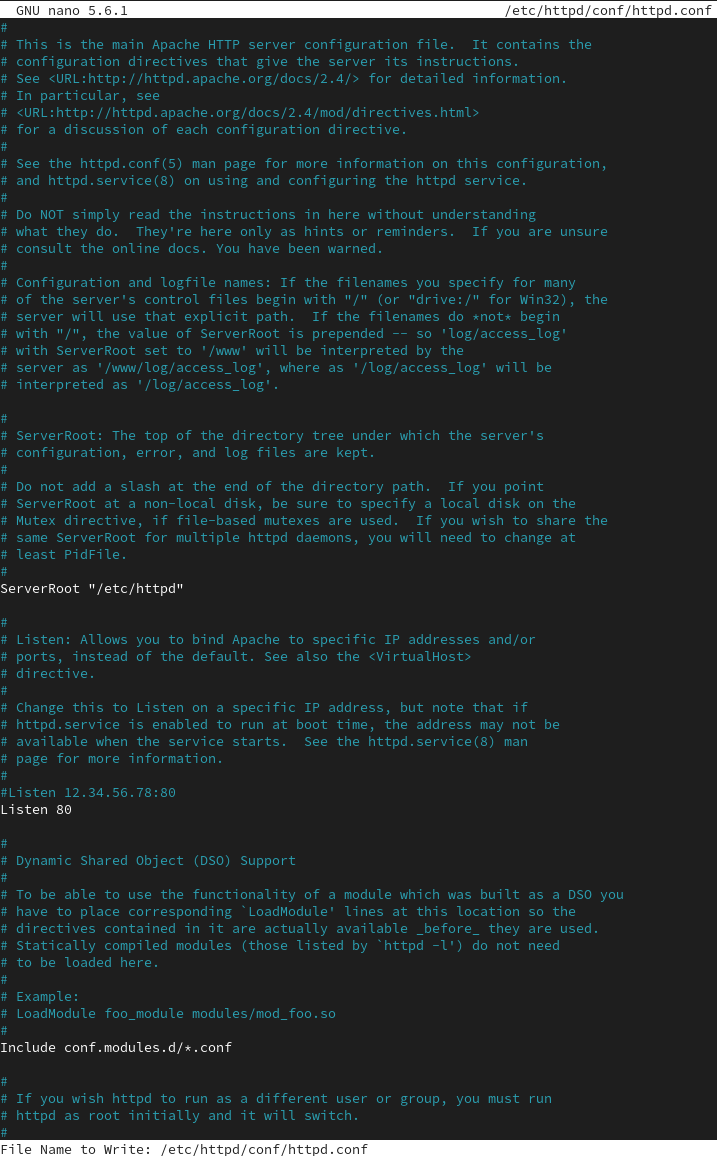
* 
* Figure 14: Список прослушиваемых портов

1. Вернем контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html: chcon -t httpd\_sys\_content\_t /var/www/html/test.html. После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. (рис. [15](#fig:16), [16](#fig:15)).

* 
* Figure 15: Обратное изменение контекста файла

* 
* Figure 16: Файл открывается

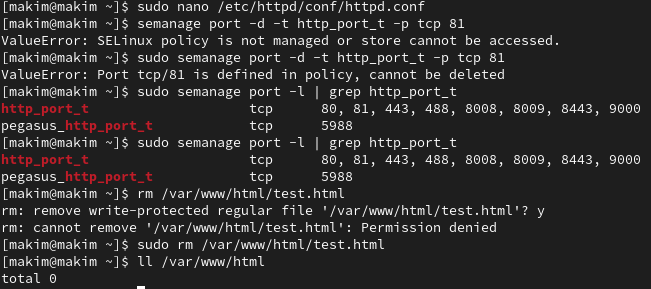
1. Исправим обратно конфигурационный файл apache, вернув Listen 80. (рис. [17](#fig:17)).

* 
* Figure 17: Обратное изменение порта

1. Удалить привязку http\_port\_t к 81 порту невозможно из-за политики (рис. [18](#fig:18)).

* Figure 18: Попытка удаления привязки TCP-порта 81
* Figure 18: Попытка удаления привязки TCP-порта 81

1. Удалим файл /var/www/html/test.html: rm /var/www/html/test.html (рис. [19](#fig:19)).

* 
* Figure 19: Удаление файла text.html

# 5 Анализ результатов

Работа выполнена без каких-либо проблем. Работа с терминалом ОС Rocky Linux в данном случае нареканий не вызвала.

# 6 Выводы

Развиты навыки администрирования ОС Linux. Полученое первое практическое знакомство с технологией SELinux. Проверена работа SELinx на практике совместно с веб-сервером Apache.

# Список литературы

1. Терминал Linux [Электронный ресурс]. URL: <{https://www.reg.ru/blog/linux-shpargalka-komandy-terminala-dlya-novichkov/}>.

2. Права доступа [Электронный ресурс]. URL: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>.

3. Дополнительные атрибуты файлов [Электронный ресурс]. Enchanted Technology, 2022. URL: <https://wiki.enchtex.info/doc/linux_file_attributes>.

4. SELinux – описание и особенности работы с системой. Часть 1 [Электронный ресурс]. Habr, 2014. URL: <https://habr.com/ru/companies/kingservers/articles/209644/>.

5. Apache [Электронный ресурс]. Skillfactory Media, 2023. URL: <https://blog.skillfactory.ru/glossary/apache/>.