Лабораторная работа №6

Дисциплина: основы информационной безопастности

Астраханцева А. А.

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 Теоретическое введение

SELinux (Security-Enhanced Linux) обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя, что превращает ее в действительно «непробиваемую» операционную систему [1].

Apache ― это программное обеспечение с открытым исходным кодом, которое позволяет создавать веб-сервер.

Веб-сервер — это программа, без которой не может работать сайт в интернете. Cайт — это набор файлов, например, HTML, CSS и JS. В каждом файле находится информация о картинках, тексте, кнопках, шрифтах и других элементах внешнего вида сайта. Все эти файлы находятся на физическом сервере, который имеет или арендует владелец сайта. Чтобы показать пользователю сайт, браузер должен связаться с сервером и получить эти файлы. Для связи с сервером браузер просит помощи у веб-сервера. Веб-сервер получает запрос от браузера, ищет ресурсы сайта и пересылает их ему. Только после этого браузер показывает контент пользователю.

Apache состоит из ядра и модулей. Ядро выполняет основные функции: обработка конфигурационных файлов, работа с протоколом HTTP, система загрузки модулей. Оно может работать самостоятельно без модулей, но тогда функционал программы будет крайне ограничен. Ядро создала команда компании Apache Software Foundation без вмешательства сторонних разработчиков. [2].

# 3 Выполнение лабораторной работы

Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus. (рис. 1)

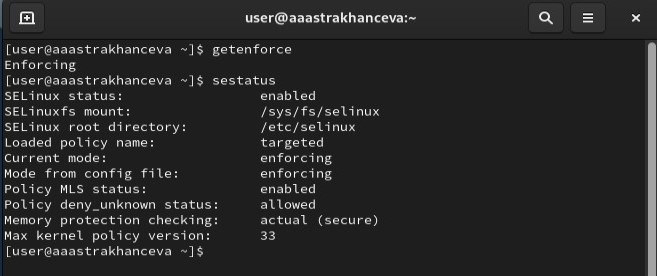


Рис. 1: Проверка работы SELinux

Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: service httpd status: (рис. 2)

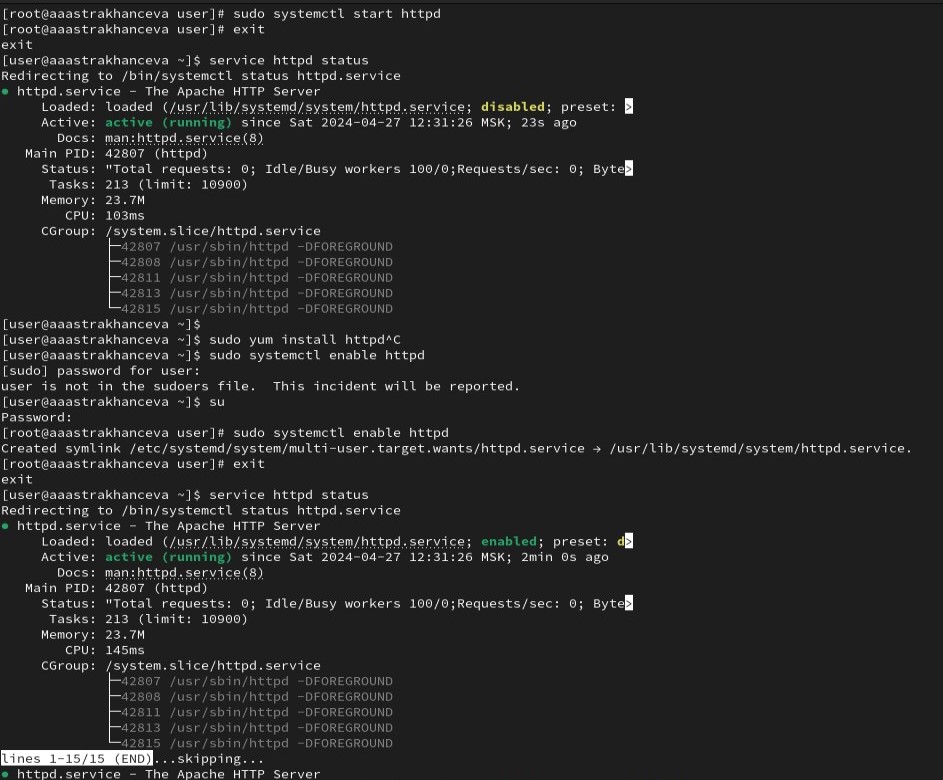


Рис. 2: Проверка работы веб-сервера

Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт (рис. 3).

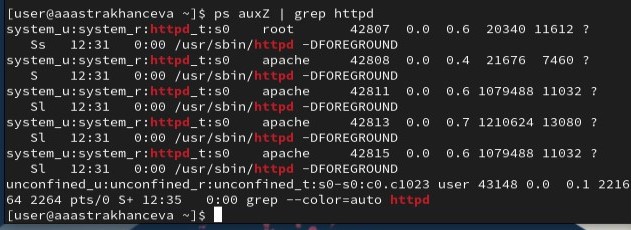


Рис. 3: Контекст безопасности веб-сервера Apache

Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды sestatus -b httpd. (рис. 4).

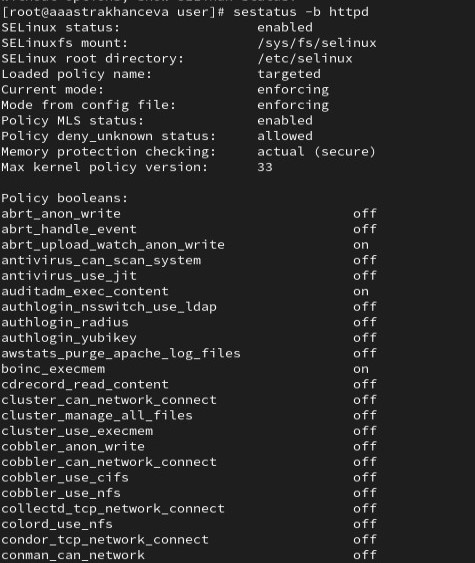


Рис. 4: Текущее состояние переключателей SELinux для Apache

Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов (рис. 5).

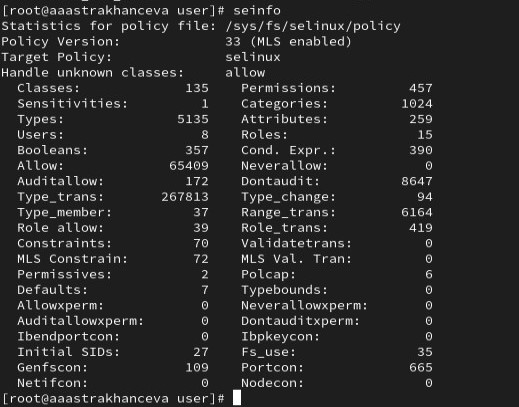


Рис. 5: Статистика по политике

Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www (2 дирректории). Определите тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html (пустая). (рис. 6).

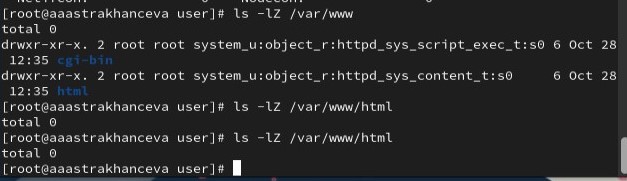


Рис. 6: Типы файлов в дирректриях /var/www и /var/www/html

Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания (рис. 7):

test

.

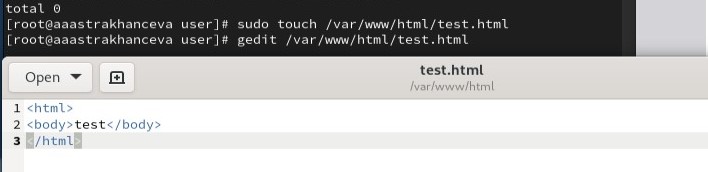


Рис. 7: Создание html-файла

Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html. (рис. 8).

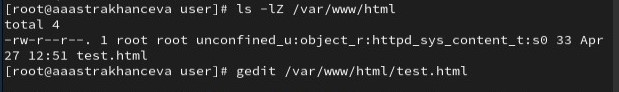


Рис. 8: Контекст файла /var/www/html

Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён. (рис. 9).

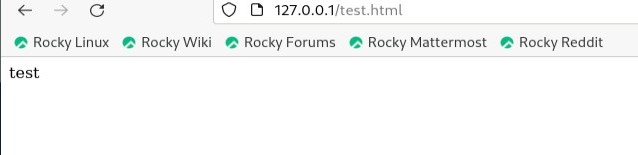


Рис. 9: Файл /var/www/html

Измените 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 проверьте, что контекст поменялся (рис. 10).



Рис. 10: Изменение контекста файла /var/www/html/test.html

Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Вы должны получить сообщение об ошибке: Forbidden You don’t have permission to access /test.html on this server (рис. 11).

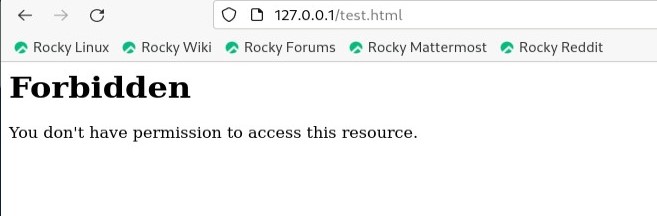


Рис. 11: Сообщение об ошибке

Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: tail /var/log/messages (рис. 12).

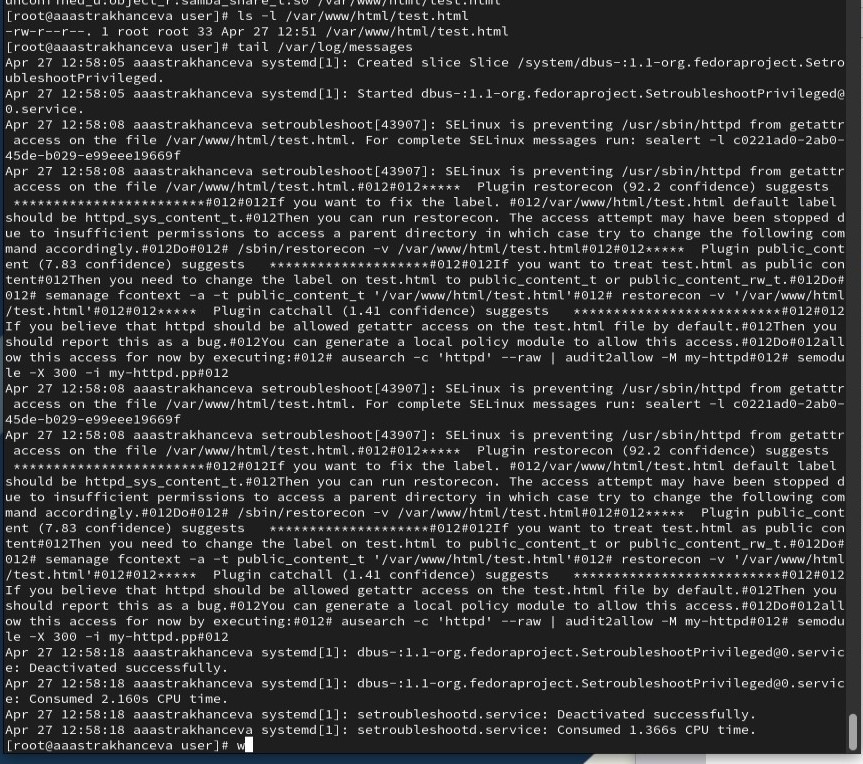


Рис. 12: Просмотр log-файлов

Попробуйте 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 найдите строчку Listen 80 и замените её на Listen 81 (рис. 13).

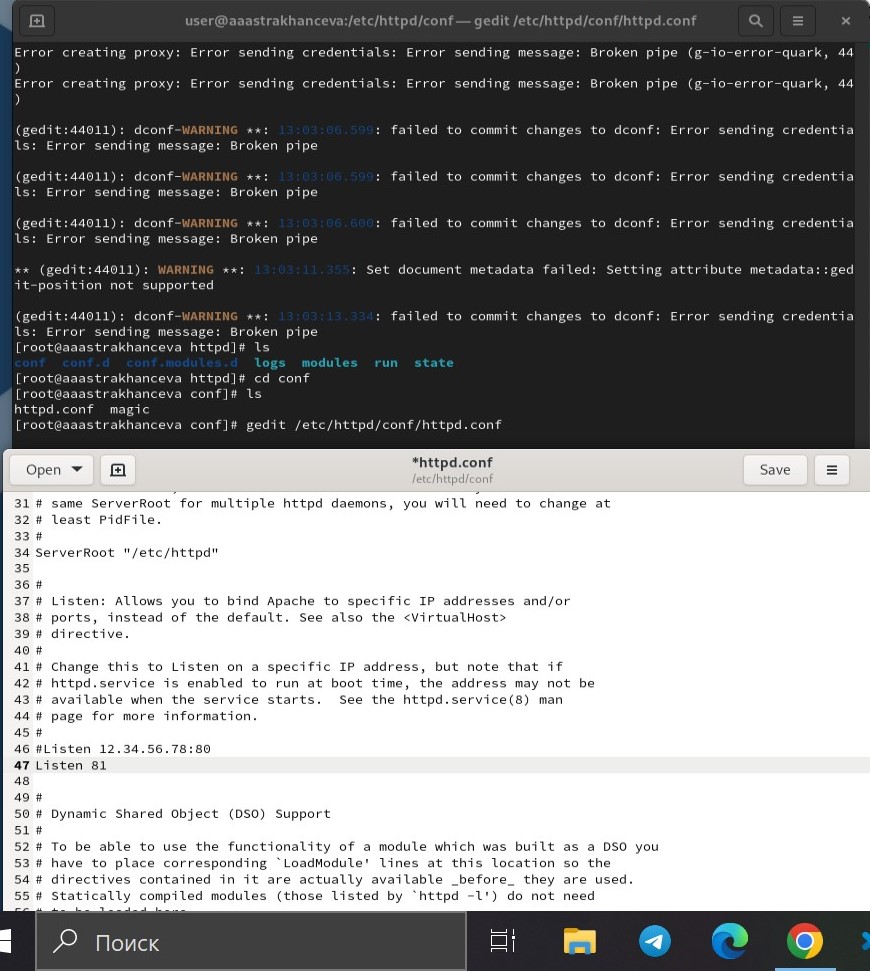


Рис. 13: Просмотр log-файлов

Проанализируйте лог-файлы: tail -nl /var/log/messages Просмотрите файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выясните, в каких файлах появились записи (рис. 14).

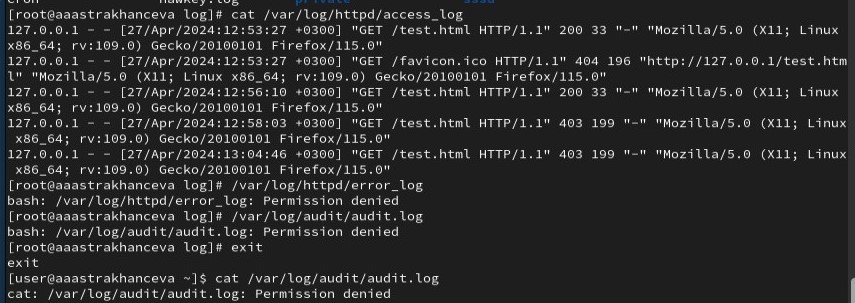


Рис. 14: Просмотр файлов /var/log/messages, /var/log/http/error\_log

Выполните команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверьте список портов командой semanage port -l | grep http\_port\_t Убедитесь, что порт 81 появился в списке (рис. 15).

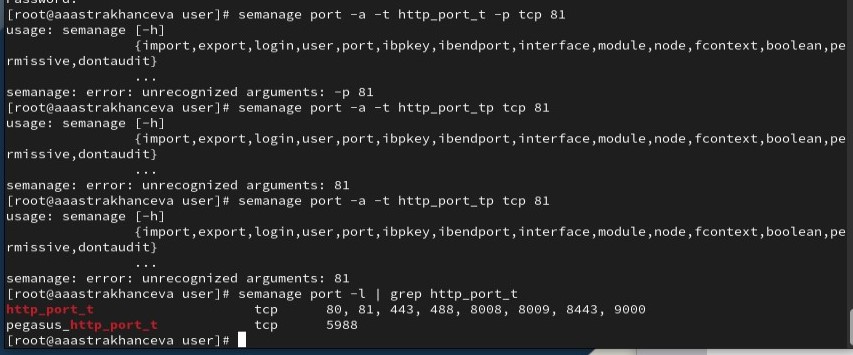


Рис. 15: Добавление порта 81

Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог? Верните 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. Вы должны увидеть содержимое файла — слово «test» (рис. 16).

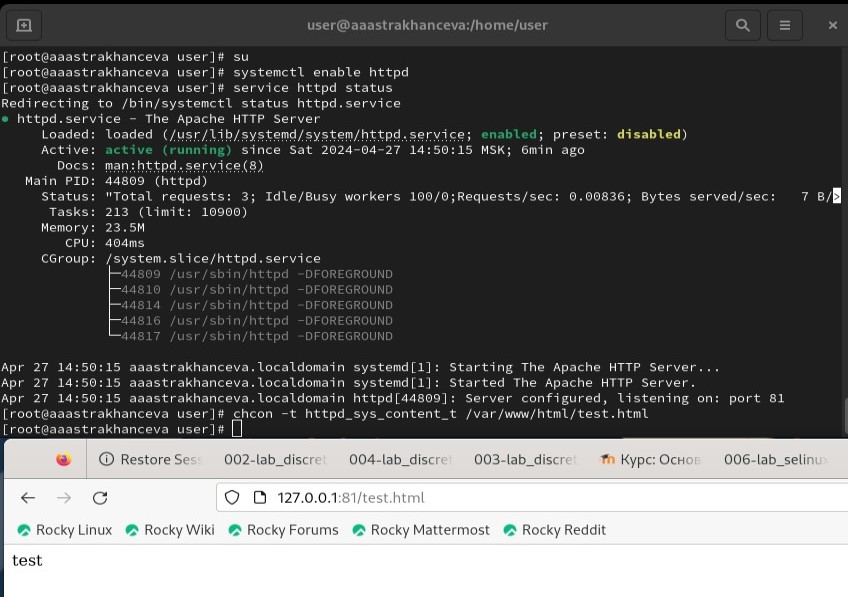


Рис. 16: Зпапуск веб-сервера Apache

Исправьте обратно конфигурационный файл apache, вернув Listen 80 (рис. 17).

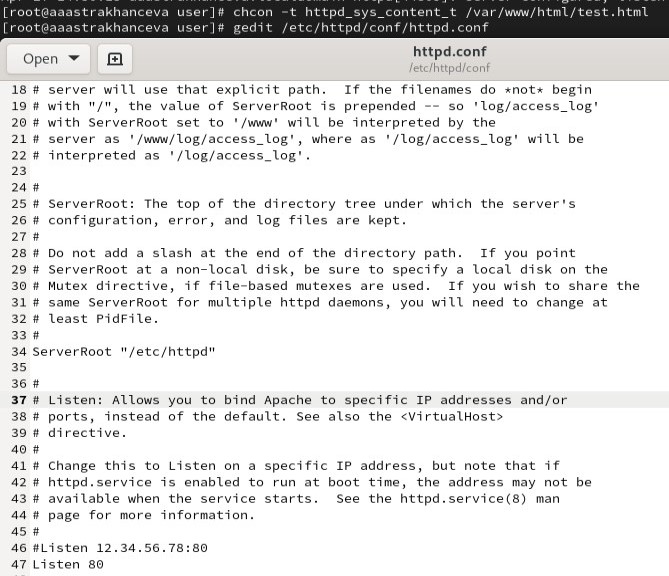


Рис. 17: Исправление конфигурационного файла apache

Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81, проверьте, что порт 81 удалён. Удалите файл /var/www/html/test.html: rm /var/www/html/test.html (рис. 18)



Рис. 18: Удаление привзяки к порту 81 и файла /var/www/html/test.html:

# 4 Выводы

В ходе выполения ЛР№6 я развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux1. Прверила работу SELinx на практике совместно с веб-сервером Apache.

# 5 Список литературы. Библиография

[1] SELinux - система принудительного контроля доступа: https://redos.red-soft.ru/base/manual/safe-redos/selinux/

[2] Права в Linux (chown, chmod, SUID, GUID, sticky bit, ACL, umask): https://habr.com/ru/articles/469667/