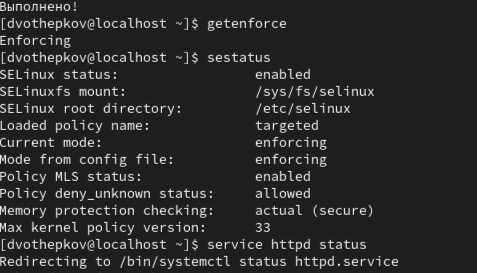
Ощепков Дмитрий Владимирович НКАбд-02-22

Дисциплина: Основы информационной безопасности

Лабораторная работа №6

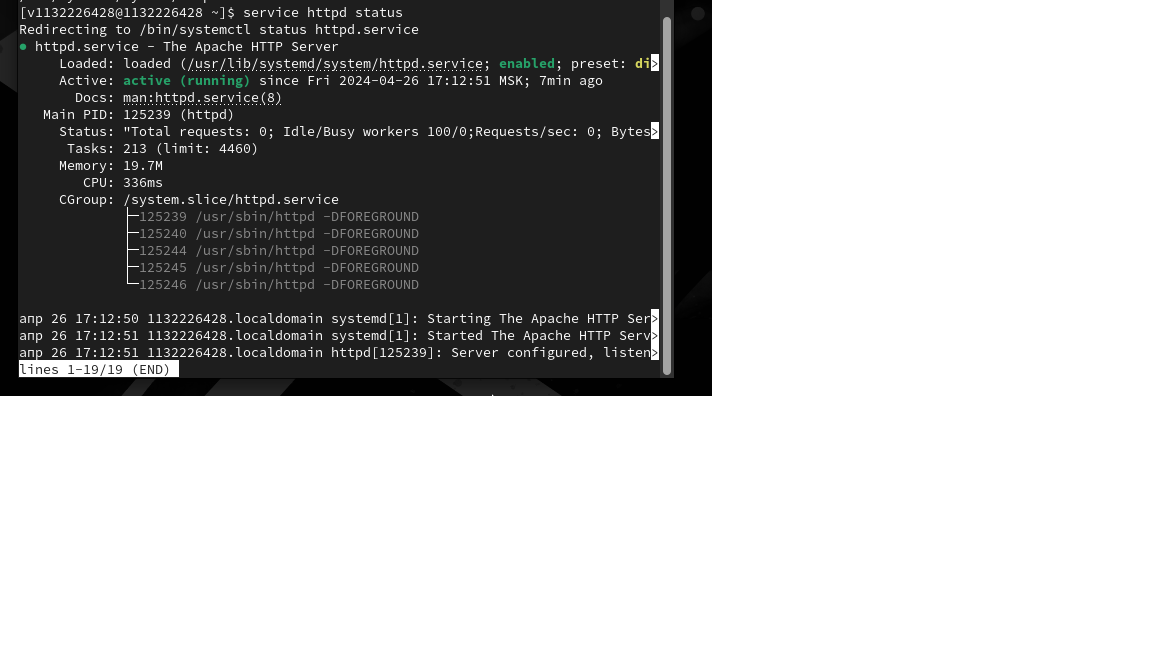
Цель работы: развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinx на практике совместно с веб-сервером Apache.

Вошел в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus

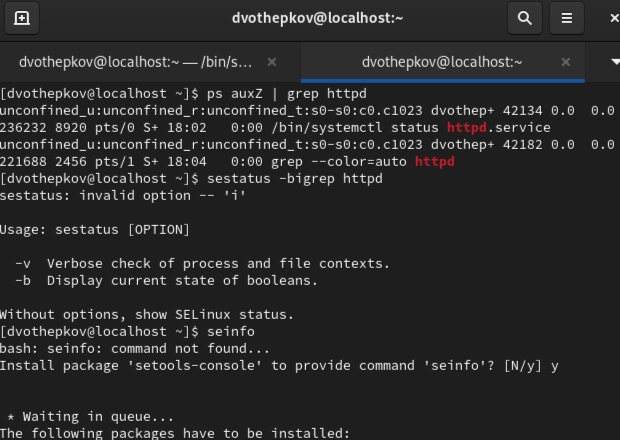


Обратился с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает:

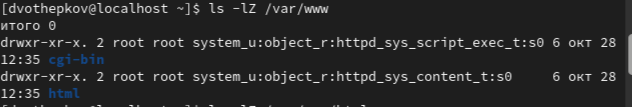




Найшел веб-сервер Apache в списке процессов, определил его контекст безопасности и занес эту информацию в отчёт.



Определил тип файлов и поддиректорий, находящихся в директории



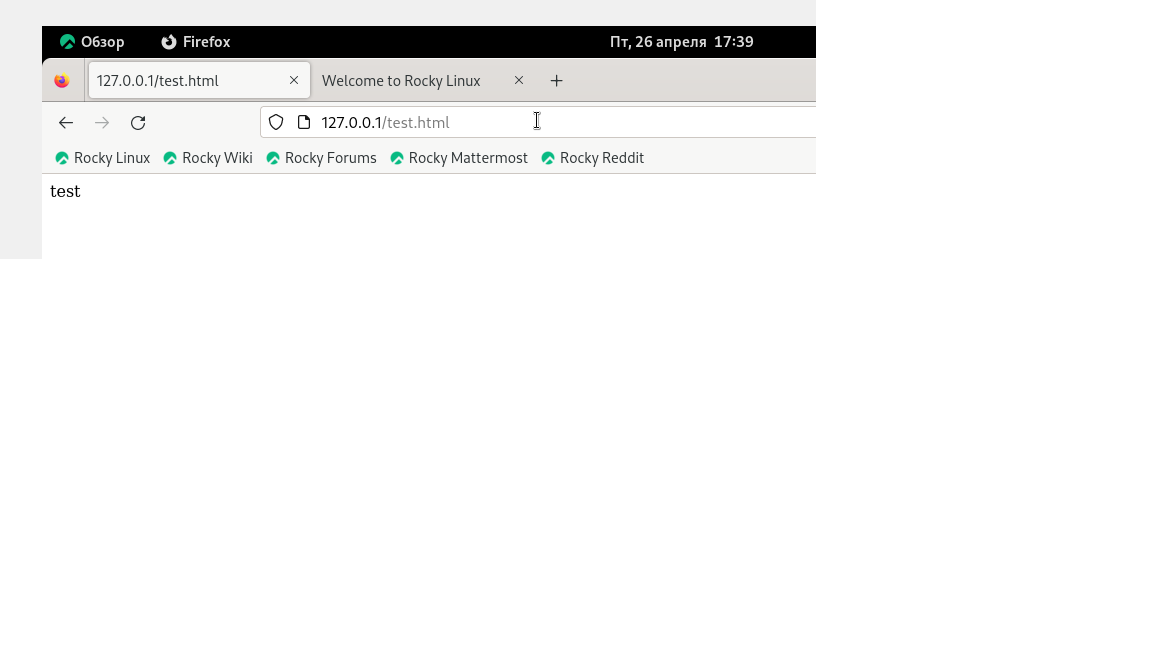
Создал от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:



Проверил контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html

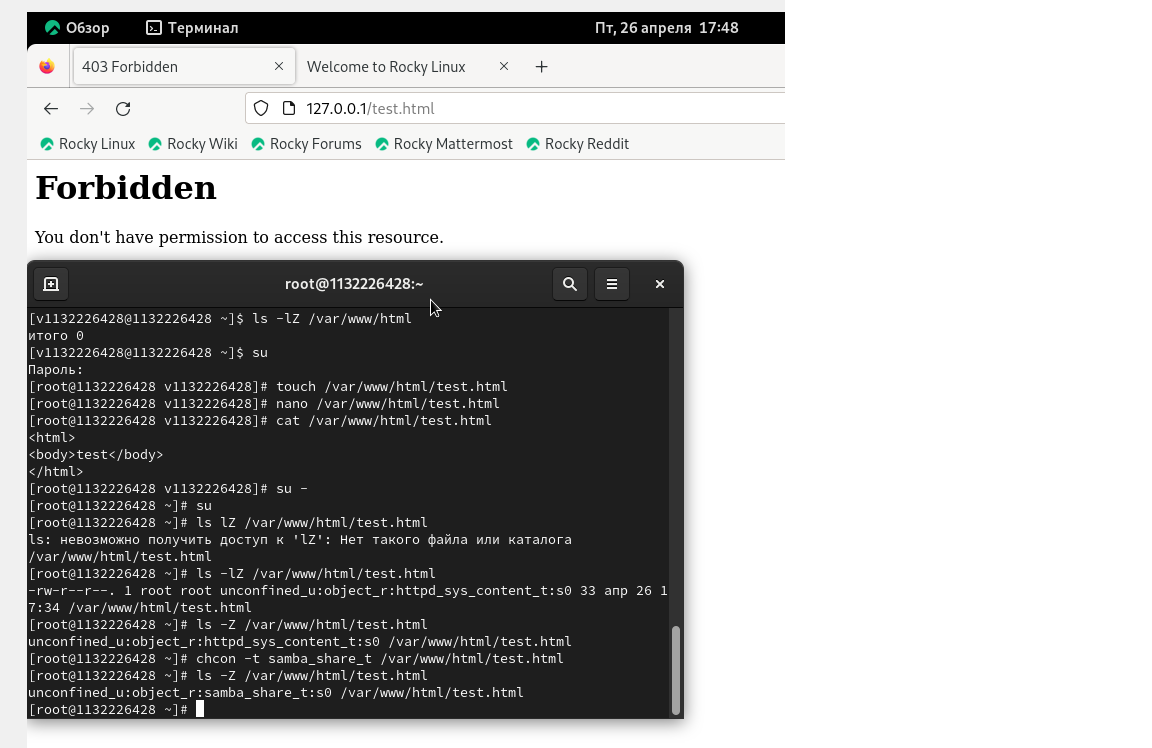


Обратился к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён

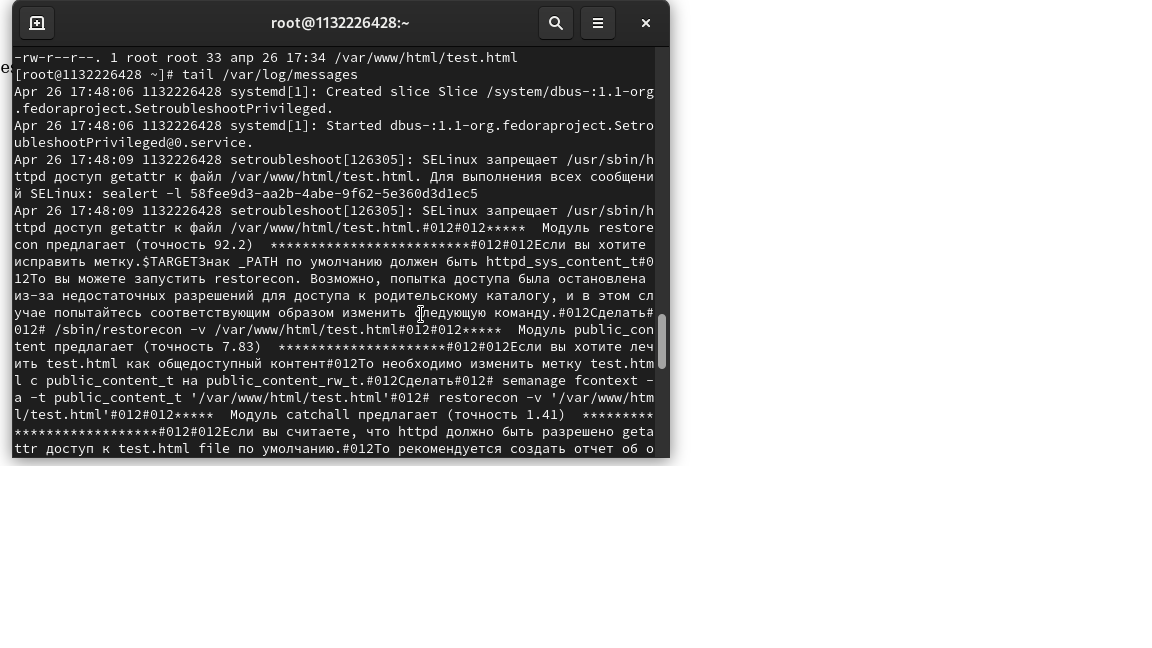


Изменил контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba\_share\_t: chcon -t samba\_share\_t /var/www/html/test.html ls -Z /var/www/html/test.html

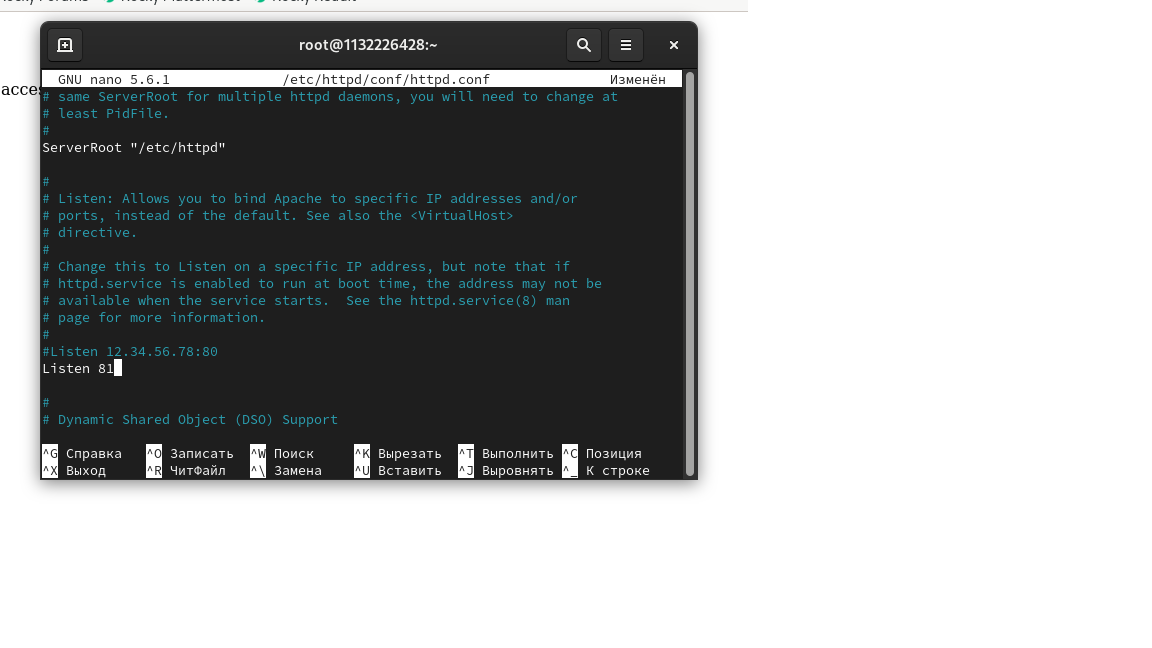
После этого проверил, что контекст поменялся. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html.



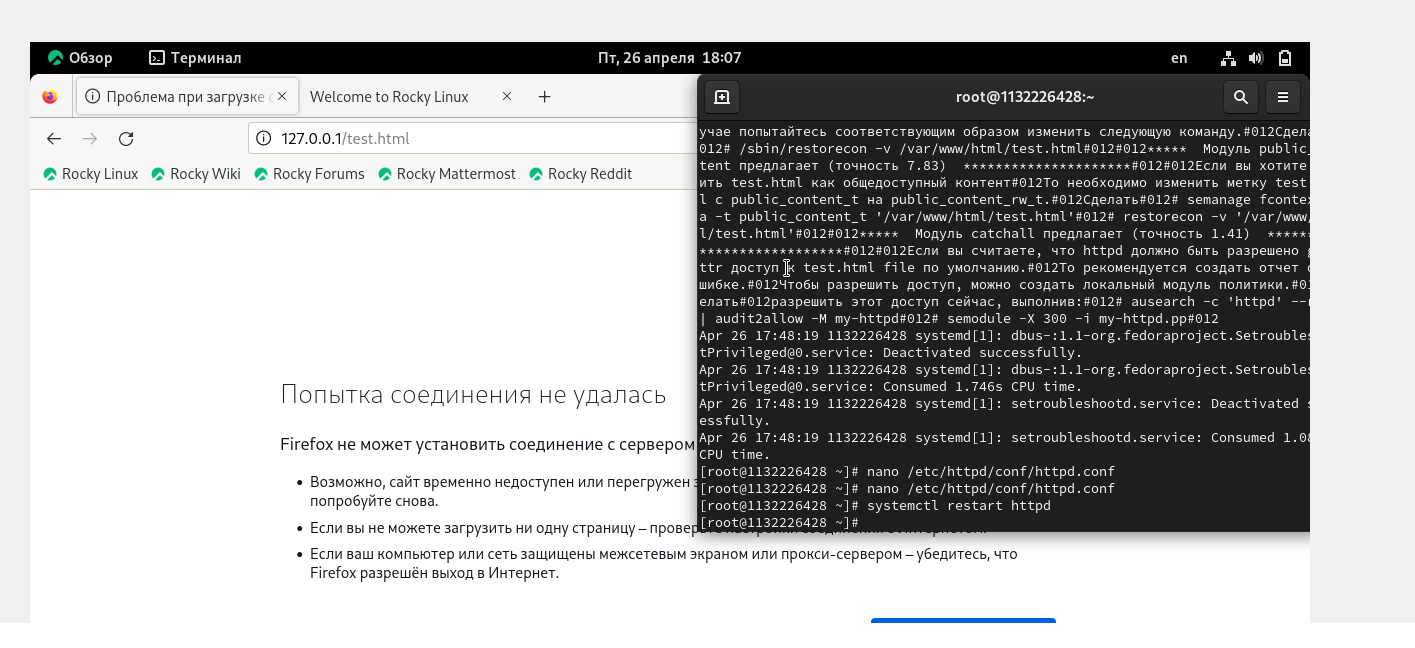
Просмотрел log-файлы веб-сервера Apache. Также просмотрел системный лог-файл:



Попробовал 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 нашел строчку Listen 80 и заменил её на Listen 81.



Выполнил перезапуск веб-сервера Apache

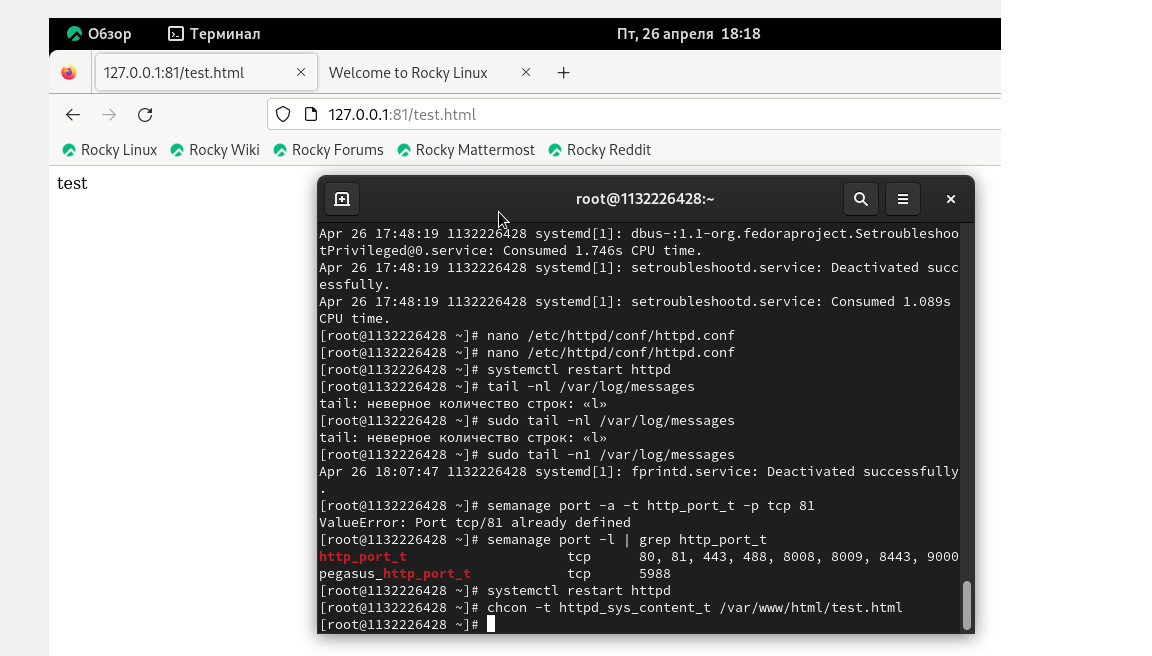


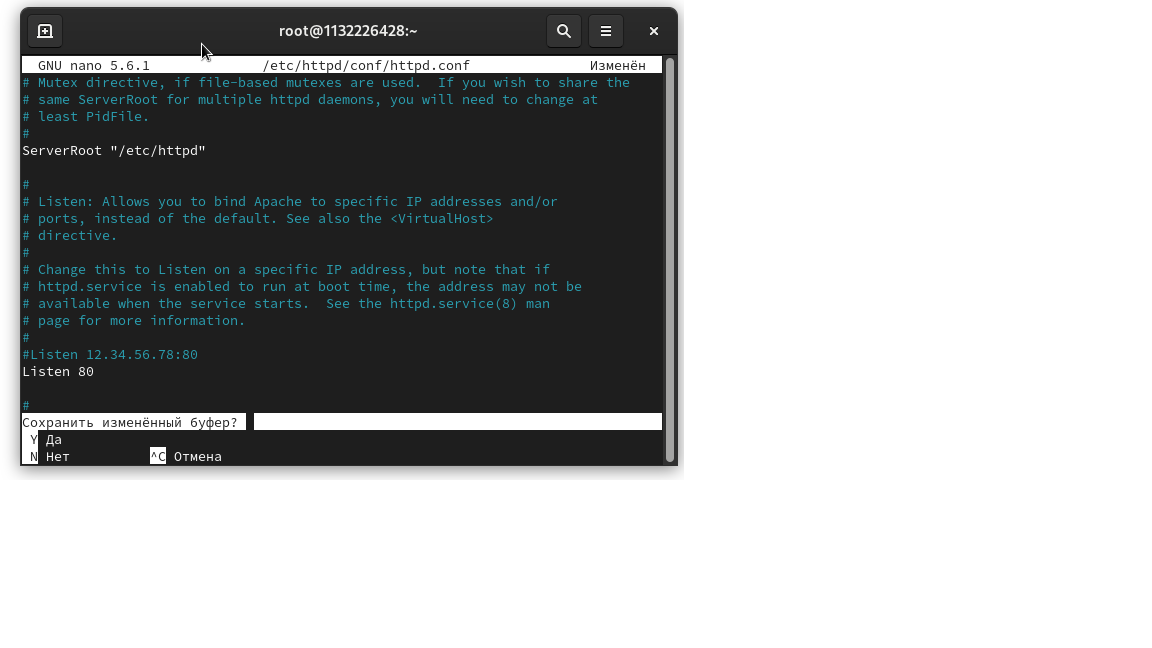
Проанализировал лог-файлы



Выполнил следующую команду







Удалил привязку http\_port\_t к 81 порту



Удалил файл



Вывод: развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinx на практике совместно с веб-сервером Apache.