Отчет по лабораторной работе №6

Мандатное разграничение прав в Linux

Динькиев Валерий

Содержание

# Цель работы

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

# Подготовка лабораторного стенда:

1. В конфигурационном файле /etc/httpd/httpd.conf задал параметр ServerName. (рис. 1).

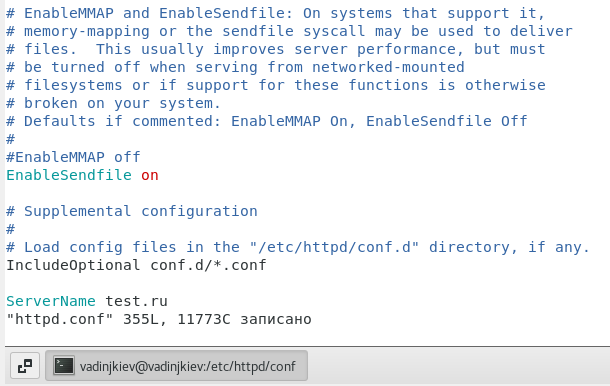


Figure 1: Параметр ServerName

1. Также проследил, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp. Отключил фильтр командами: iptables -F, iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT. Так же добавил разрешающие правила. (рис. 2), (рис. 3), (рис. 4).

Figure 2: Отключение фильтра

Figure 2: Отключение фильтра

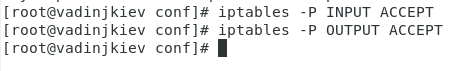


Figure 3: Отключение фильтра

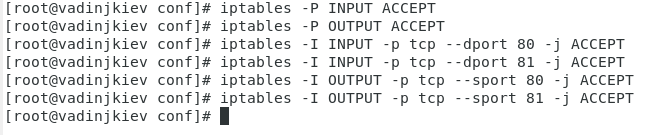
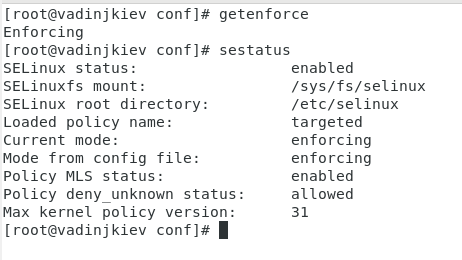


Figure 4: Добавление разрешающих правил

# Выполнение лабораторной работы

1. Вошел в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus.(рис. **¿fig:005?**).



1. Обратился с помощью браузера к веб-серверу, запущенному на компьютере, и убедился, что последний работает: service httpd status(рис. 5), (рис. 6).

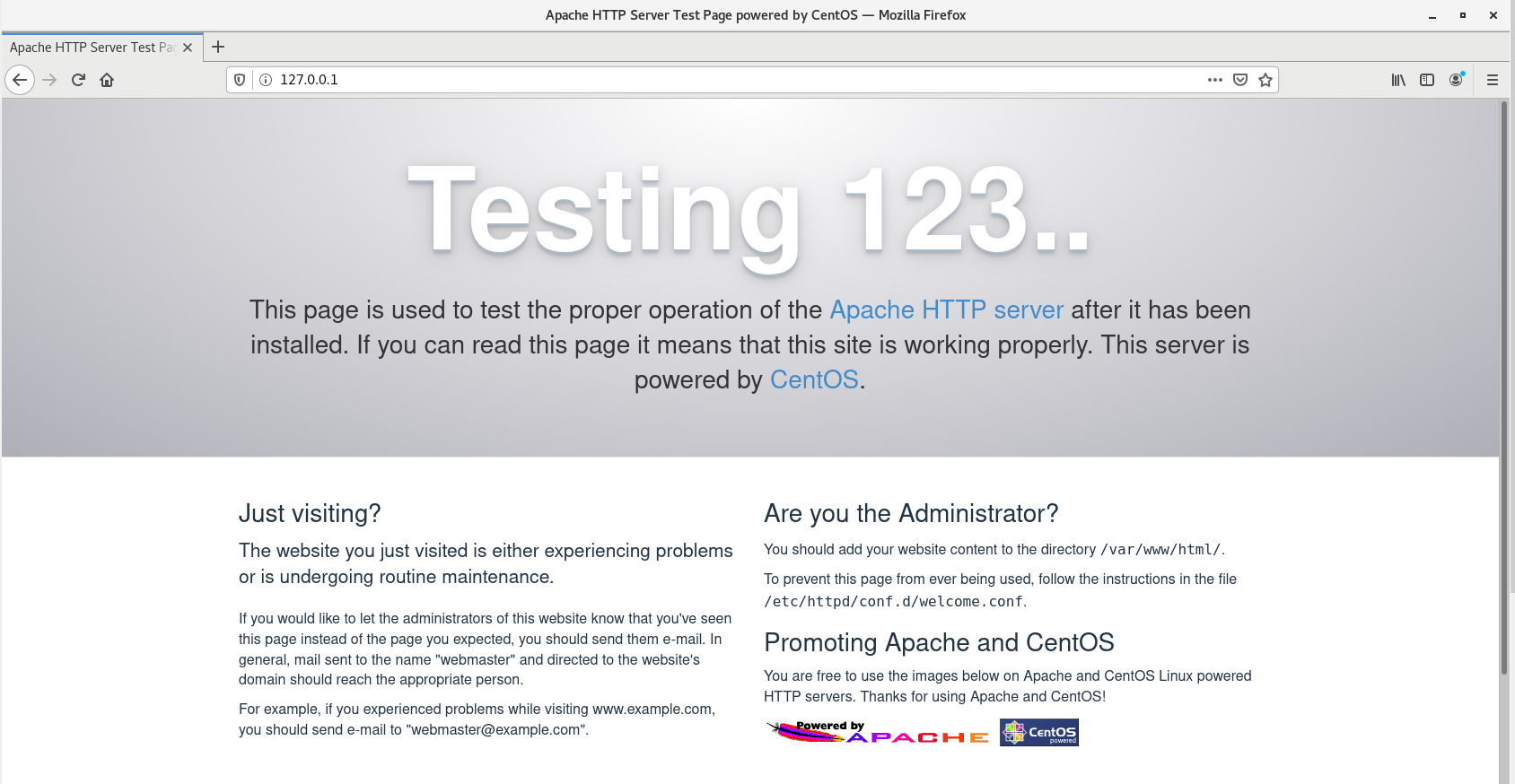


Figure 5: Проверка через браузер

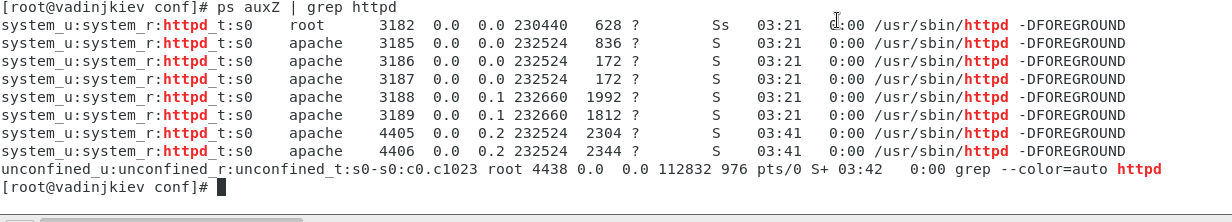


Figure 6: Проверка статуса

1. Нашел веб-сервер Apache в списке процессов, определил его контекст безопасности. (рис. 7).

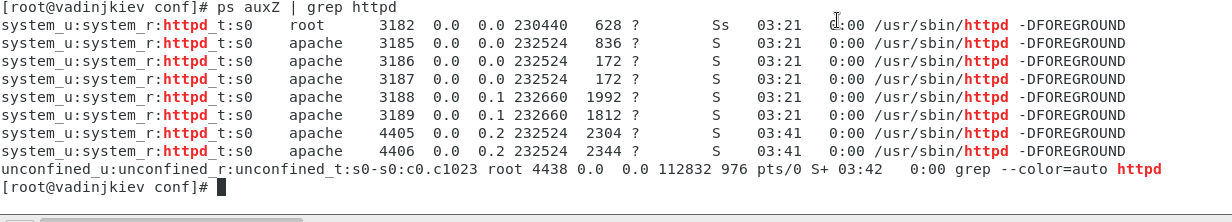


Figure 7: веб-сервер Apache

1. Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды: sestatus -bigrep httpd. Обратил внимание, что многие из них находятся в положении «off». (рис. 8).

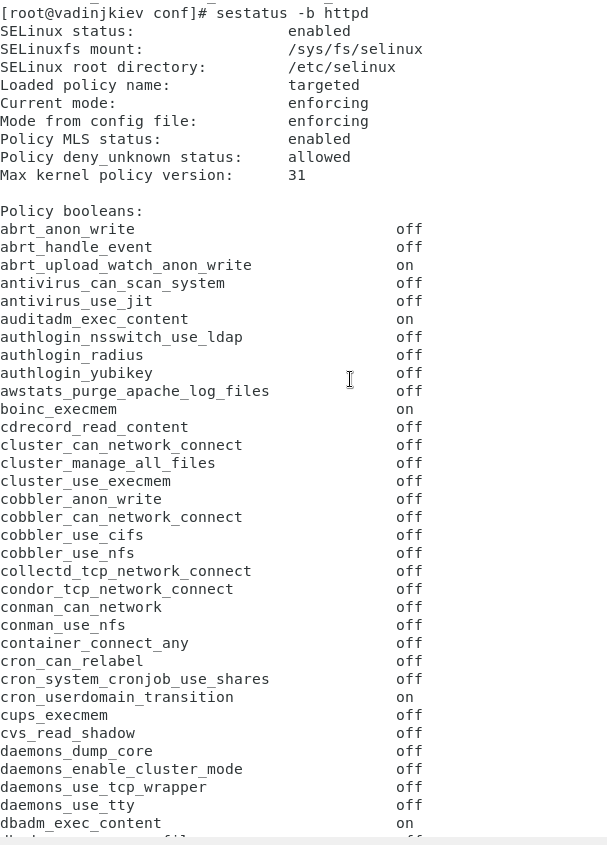


Figure 8: Просмотр переключателей SELinux для Apache

1. Посмотрел статистику по политике с помощью команды seinfo, также определил множество пользователей(8), ролей(14), типов(4793) (рис. 9).

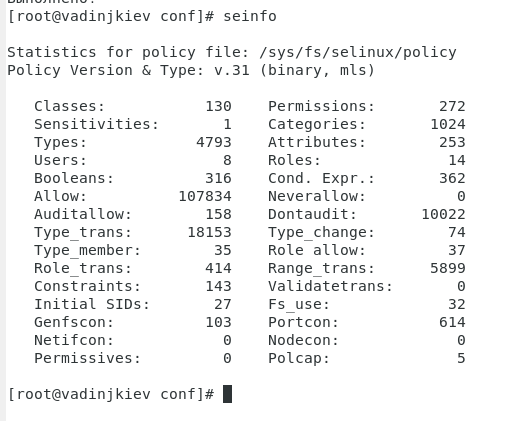


Figure 9: Статистика

1. Определил тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды: ls -lZ /var/www.
2. Определил тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html.
3. Определил круг пользователей, которым разрешено создание файлов в директории /var/www/html. (рис. 10).

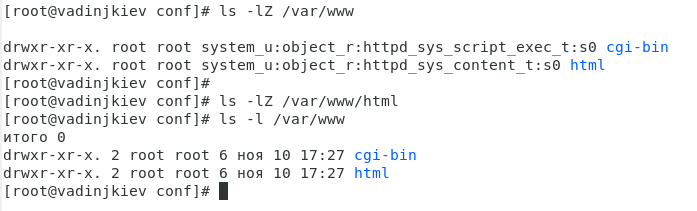


Figure 10: Статистика

1. Создал от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html(рис. 11).

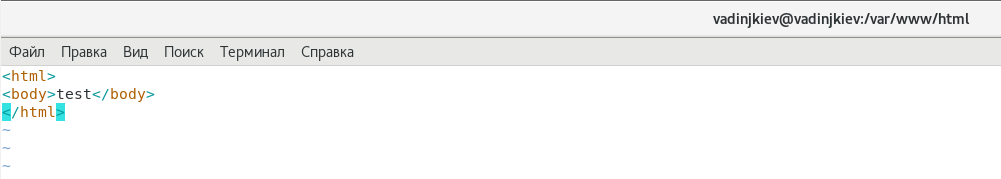


Figure 11: Создание файла

1. Проверил контекст созданного файла. httpd\_sys\_content\_t (рис. 12).

Figure 12: Проверка

Figure 12: Проверка

1. Обратился к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедился, что файл был успешно отображён. (рис. 13).

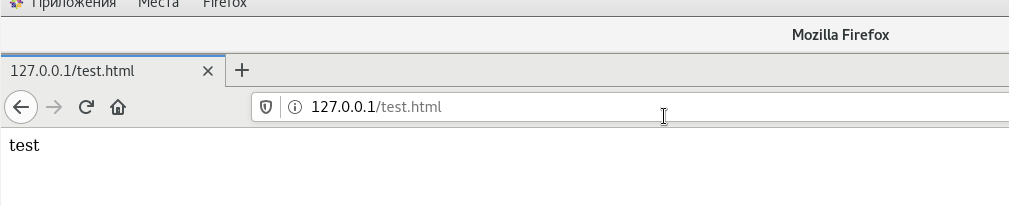


Figure 13: Получение доступа к файлу через браузер

1. Проверил контекст файла командой: ls -Z /var/www/html/test.html (рис. 14).
2. Изменил контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t. После этого проверил, что контекст поменялся. (рис. 14).

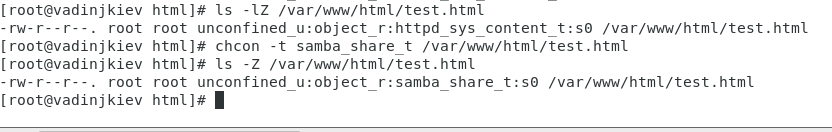


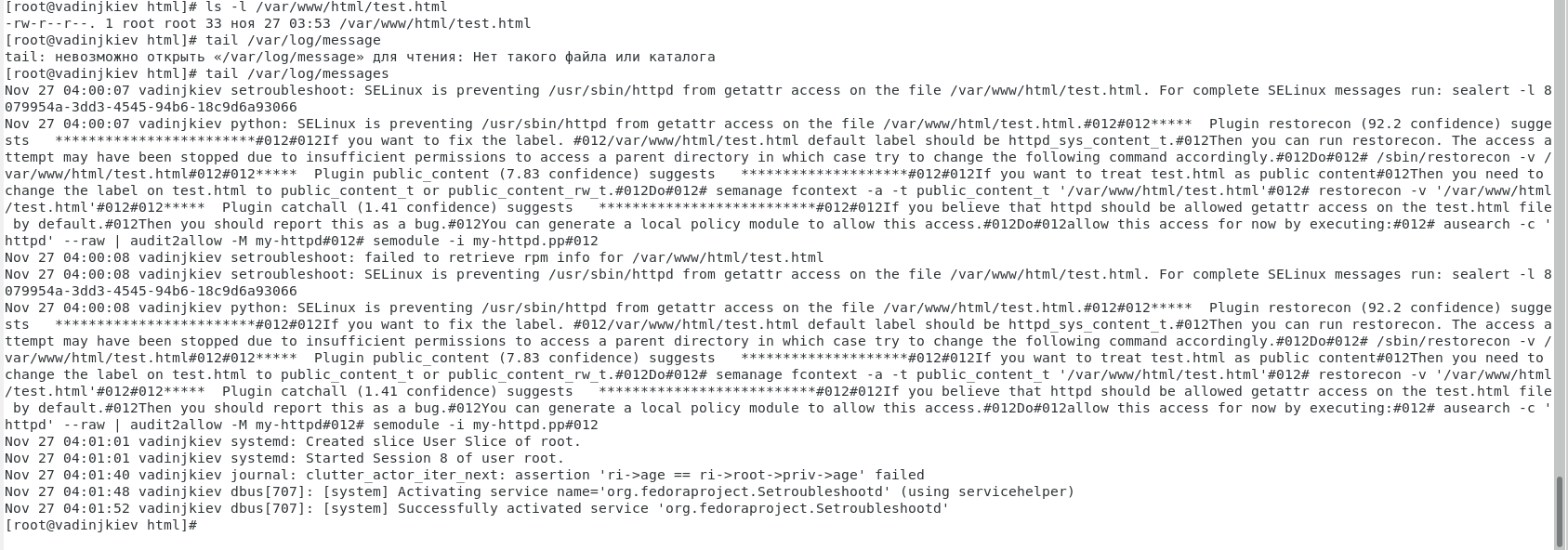
Figure 14: Изменение контекста, проверка

1. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Получил сообщение об ошибке. (рис. 15).



Figure 15: Получение доступа к файлу через браузер

1. Проанализировал ситуацию. Файл не был отображён потому что мы изменили контекст файла. Просмотрел log-файлы веб-сервера Apache. Также просмотрел системный лог-файл: tail /var/log/messages (рис. **¿fig:017?**).



1. 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.(рис. 16).

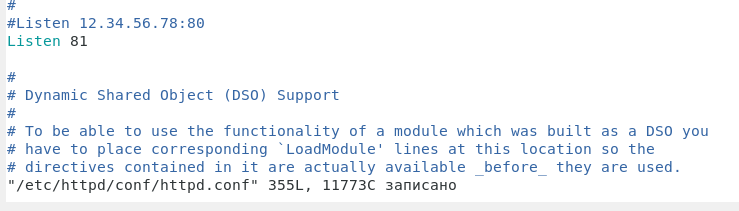


Figure 16: Изменеие порта 80 на 81

1. Проанализиировал лог-файлы. Просмотрел файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log. (рис. 17), (рис. 18), (рис. 19), (рис. 20).

Figure 17: Анализ лог-файла

Figure 17: Анализ лог-файла

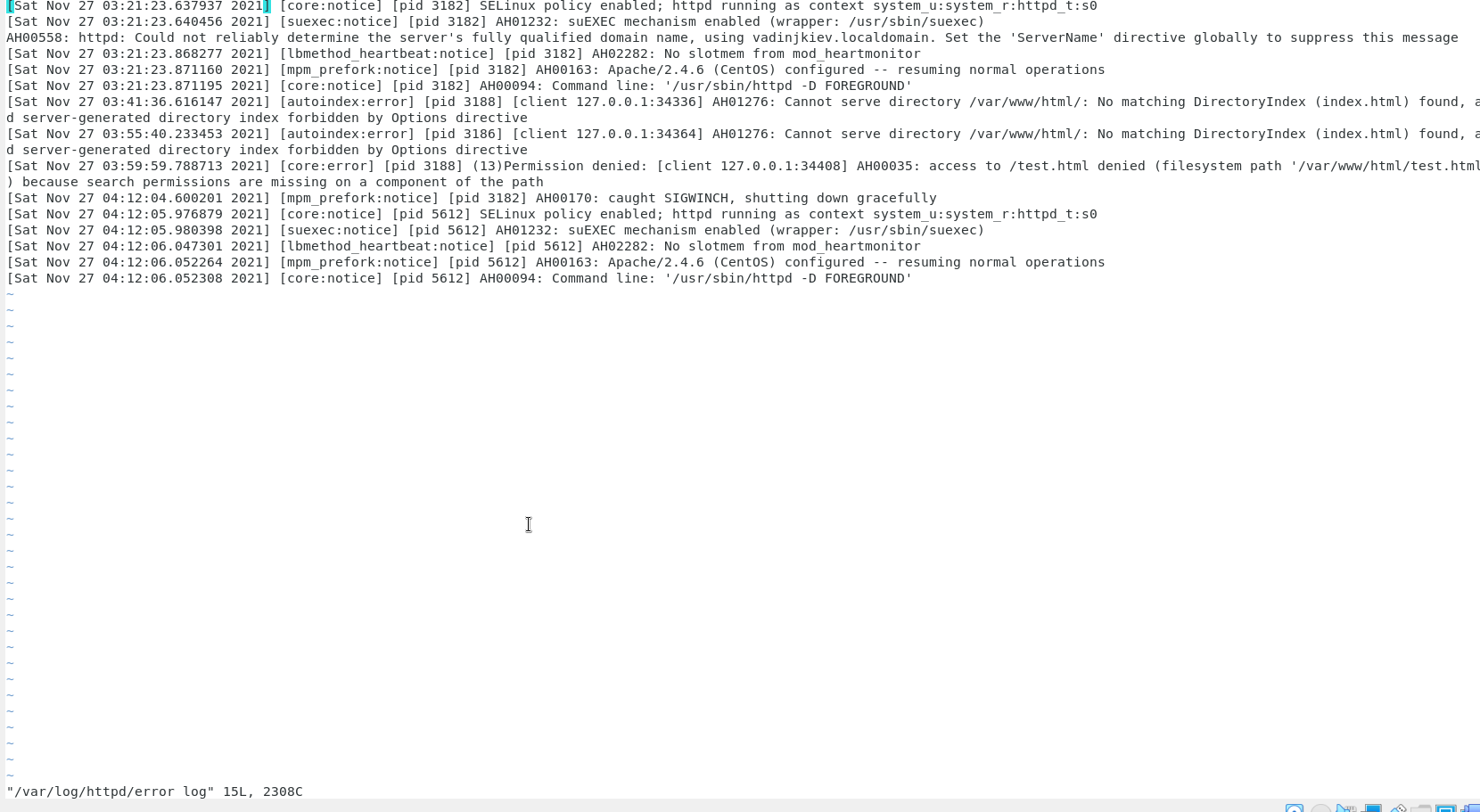


Figure 18: Просмотр файла /var/log/http/error\_log

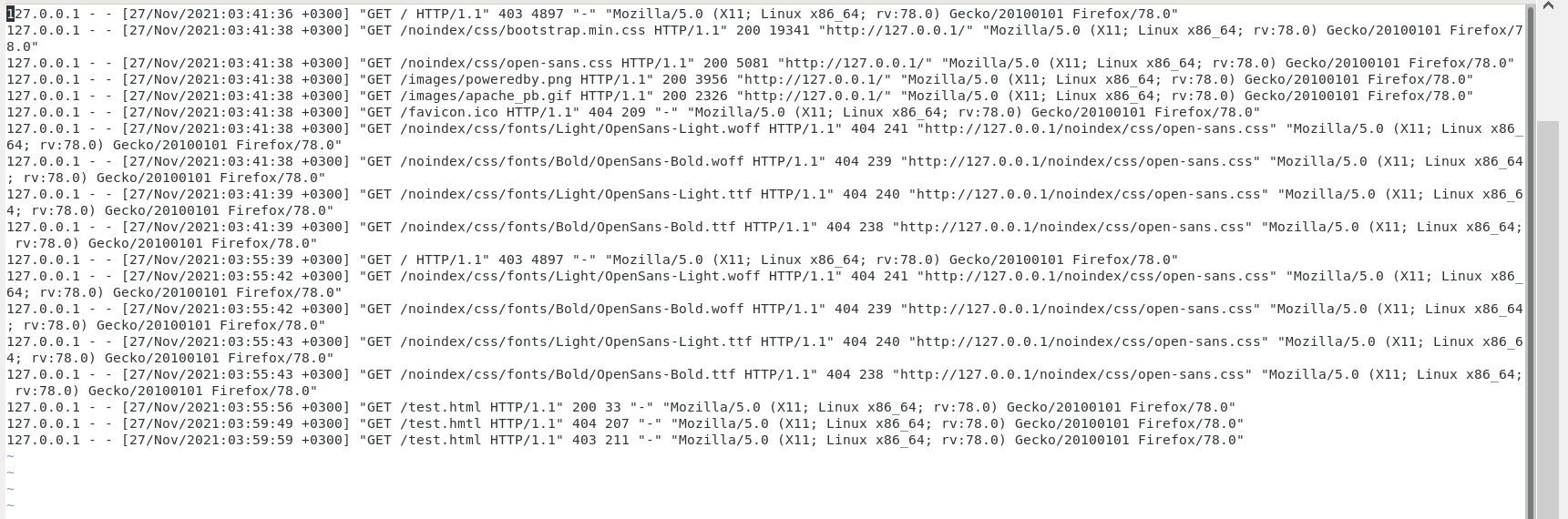


Figure 19: Просмотр файла /var/log/http/access\_log

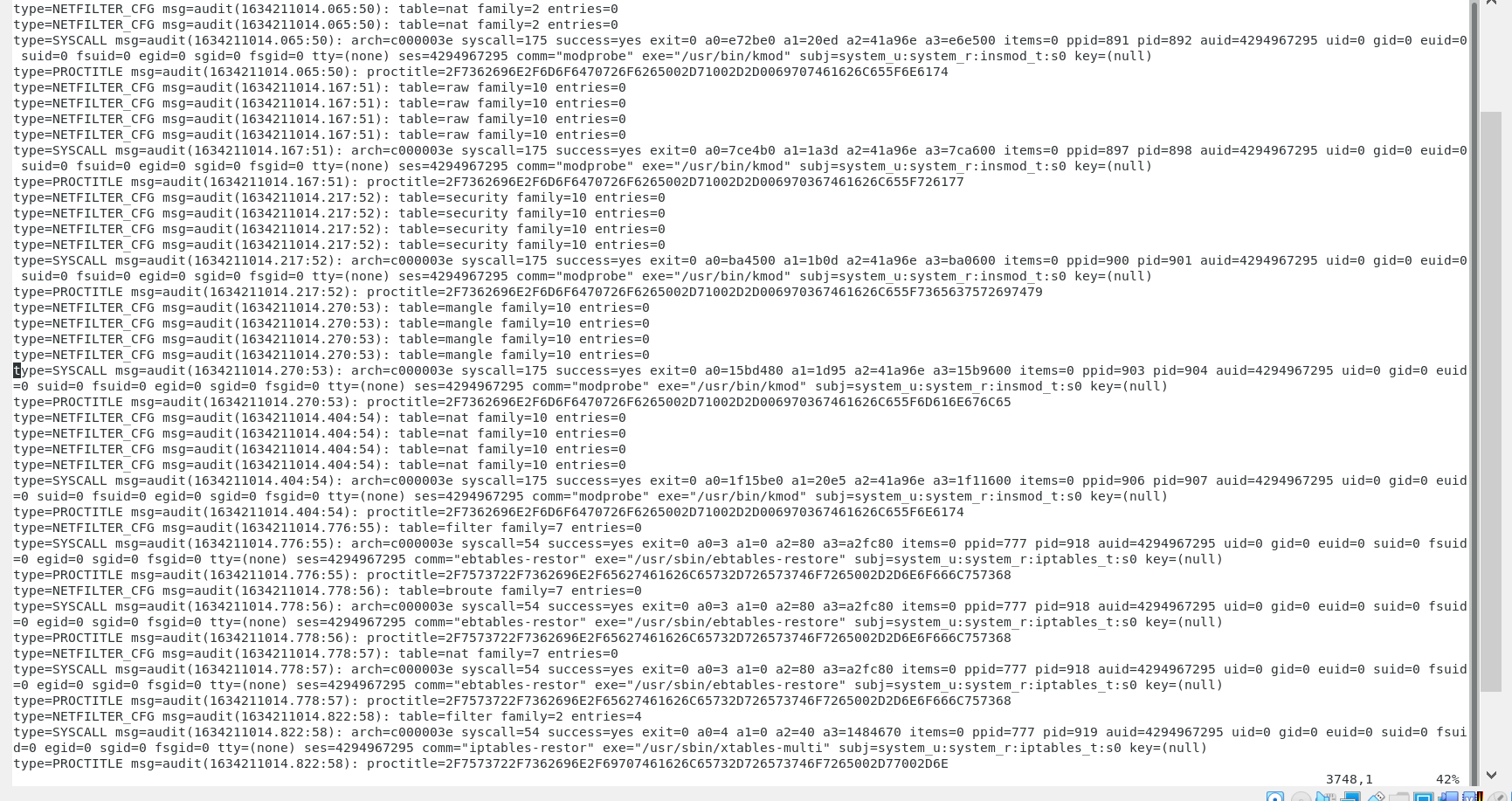


Figure 20: Просмотр файла var/log/audit/audit.log

1. Выполнил команду: semanage port -a -t http\_port\_t -р tcp 81. После этого проверил список портов командой: semanage port -l | grep http\_port\_t. Убедился, что порт 81 появился в списке. (рис. 21).

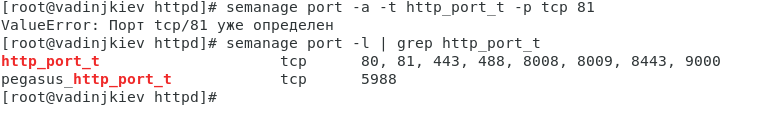


Figure 21: Выполнение и проверка

1. Вернул 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 попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Увидели содержимое файла — слово «test». (рис. 22), (рис. 23).

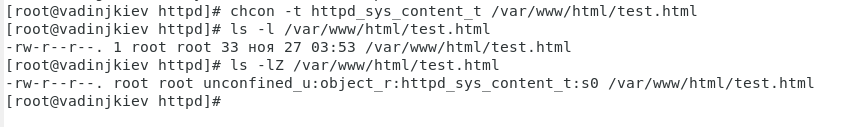


Figure 22: Возвращение контекста



Figure 23: Получение доступа к файлу через браузер

1. Исправил обратно конфигурационный файл apache, вернув Listen80. (рис. 24).

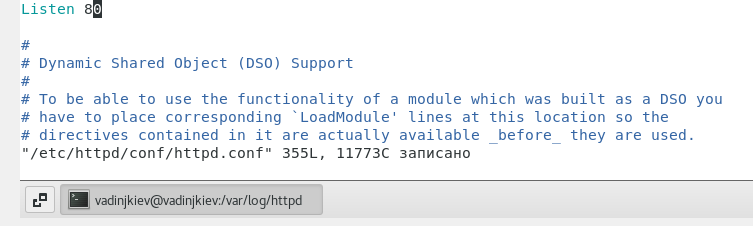


Figure 24: Исправленный файл apache

1. Удалил привязку http\_port\_t к 81 порту. (рис. 25).

Figure 25: Удаление привязки к 81 порту

Figure 25: Удаление привязки к 81 порту

1. Удалил файл /var/www/html/test.html. (рис. 26).

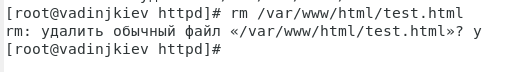


Figure 26: Удаление файла /var/www/html/test.html

# Выводы

На основе проделанной работы развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinx на практике совместно с веб-сервером Apache.