Отчёт по лабораторной работе №6

Основы информационной безопасности

Надежда Александровна Рогожина

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 (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена. Эти улучшения позволили SELinux стать универсальной системой, способной эффективно решать массу актуальных задач. Стоит помнить, что классическая система прав Unix применяется первой, и управление перейдет к SELinux только в том случае, если эта первичная проверка будет успешно пройдена.

Для того, чтобы понять, в чем состоит практическая ценность SELinux, рассмотрим несколько примеров, когда стандартная система контроля доступа недостаточна. Если SELinux отключен, то вам доступна только классическая дискреционная система контроля доступа, которая включает в себя DAC (избирательное управление доступом) или ACL(списки контроля доступа). То есть речь идет о манипулировании правами на запись, чтение и исполнение на уровне пользователей и групп пользователей, чего в некоторых случаях может быть совершенно недостаточно. Например:

* Администратор не может в полной мере контролировать действия пользователя. Например, пользователь вполне способен дать всем остальным пользователям права на чтение собственных конфиденциальных файлов, таких как ключи SSH.
* Процессы могут изменять настройки безопасности. Например, файлы, содержащие в себе почту пользователя должны быть доступны для чтения только одному конкретному пользователю, но почтовый клиент вполне может изменить права доступа так, что эти файлы будут доступны для чтения всем.
* Процессы наследуют права пользователя, который их запустил. Например, зараженная трояном версия браузера Firefox в состоянии читать SSH-ключи пользователя, хотя не имеет для того никаких оснований.

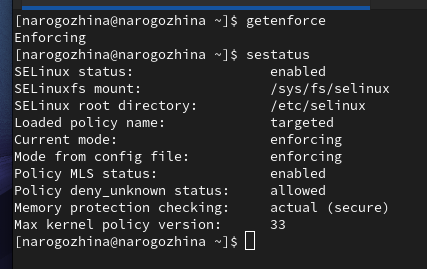
По сути, в традиционной модели избирательного управления доступом (DAC), хорошо реализованы только два уровня доступа — пользователь и суперпользователь. Нет простого метода, который позволил бы устанавливать для каждого пользователя необходимый минимум привилегий. В табл. [[1](#tbl:std-dir)] приведено краткое описание основных терминов SELinux.

Table 1: Описание основных терминов SELinux

| Термин | Описание |
| --- | --- |
| Домен | Список действий, которые может выполнять процесс. Обычно в качестве домена определяется минимально-возможный набор действий, при помощи которых процесс способен функционировать. Таким образом, если процесс дискредитирован, злоумышленнику не удастся нанести большого вреда. |
| Роль | Список доменов, которые могут быть применены. Если какого-то домена нет в списке доменов какой-то роли, то действия из этого домена не могут быть применены. |
| Тип | Набор действий, которые допустимы по отношения к объекту. Тип отличается от домена тем, что он может применяться к пайпам, каталогам и файлам, в то время как домен применяется к процессам. |
| Контекст безопасности | Все атрибуты SELinux — роли, типы и домены. |

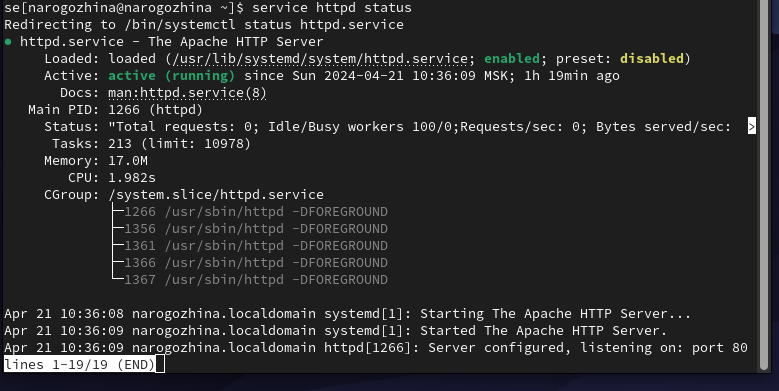
# 3 Выполнение лабораторной работы

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



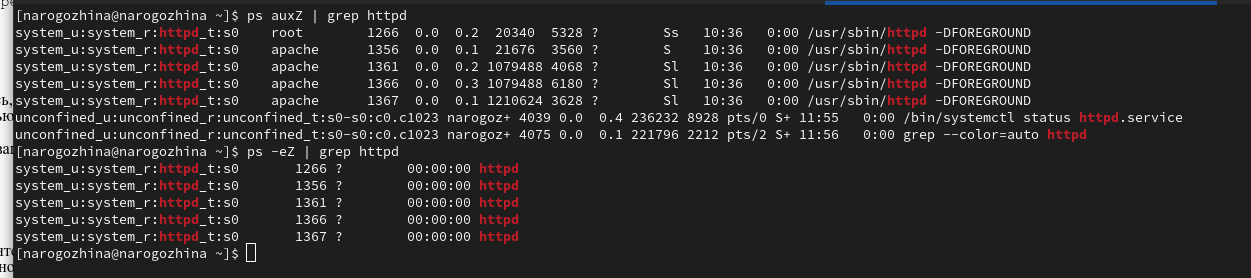
Статус SELinux

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



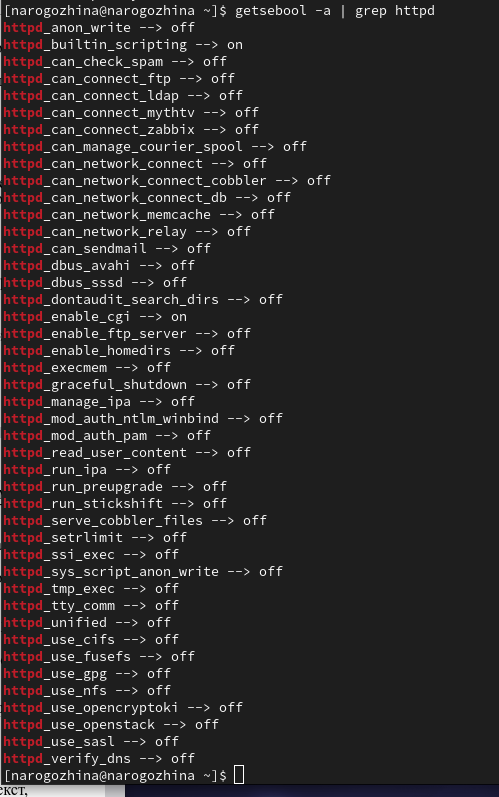
service httpd status

1. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду ps auxZ | grep httpd или ps -eZ | grep httpd (рис. [??]).



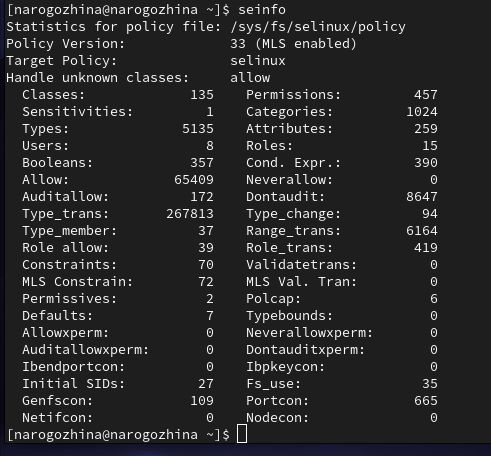
обе команды

1. Посмотрите текущее состояние переключателей SELinux для Apache (рис. [??]).



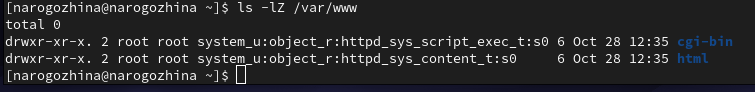
Состояние переключателей SELinux

1. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов (рис. [??]).



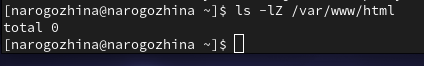
Статистика по политике

1. Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www (рис. [??]).



Тип файлов и поддиректорий

1. Определите тип файлов, находящихся в директории /var/www/html ls -lZ /var/www/html (рис. [??]).

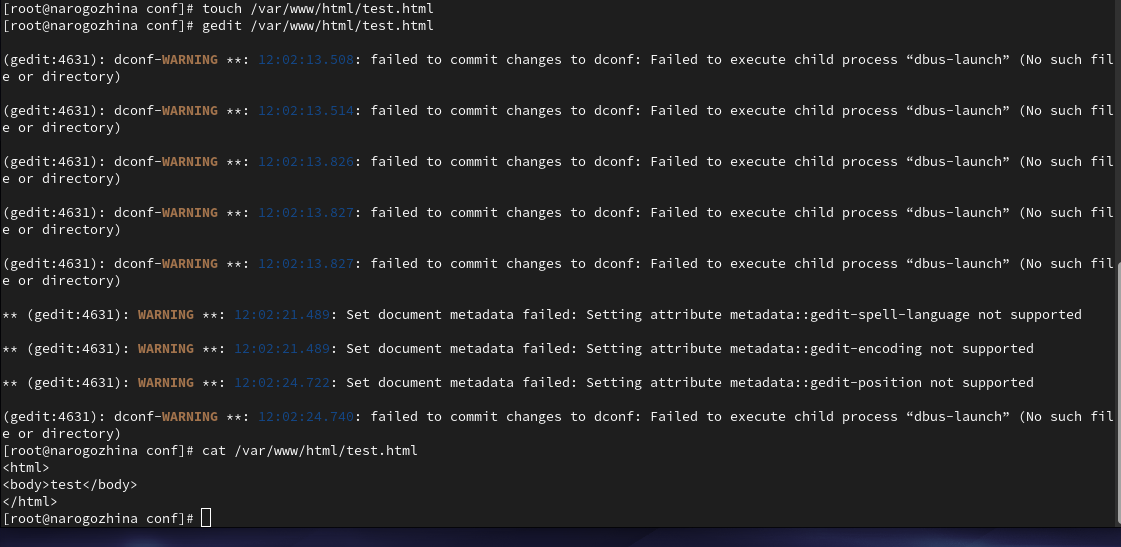


Поддиректории

1. Создание файлов в директории /var/www/html разрешено только владельцу данной директории.
2. 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:

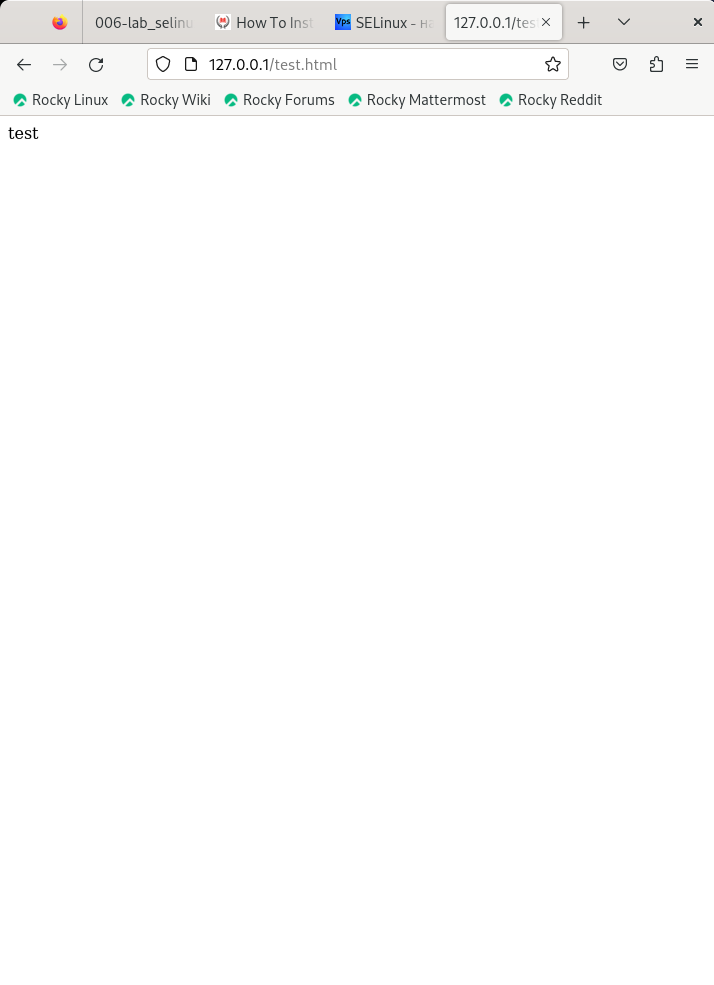
<html>  
<body>test</body>  
</html>

(рис. [??]).



Создание файла

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

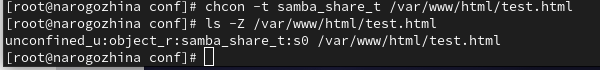


test.ru

1. Тип файла test.html: unconfined\_u:object\_r:httpd\_sys\_content\_t:s0
2. 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

(рис. [??]).

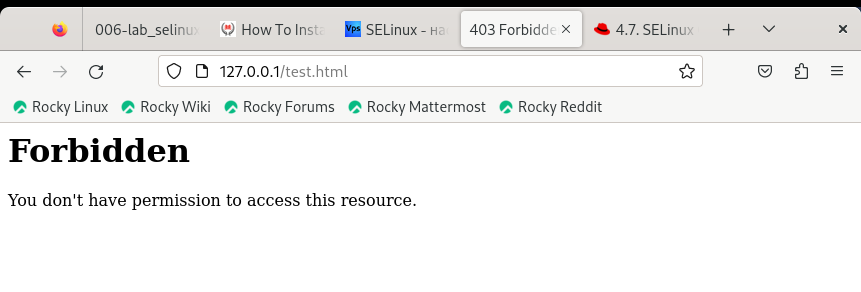


изменение контекста

1. 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. [??]).



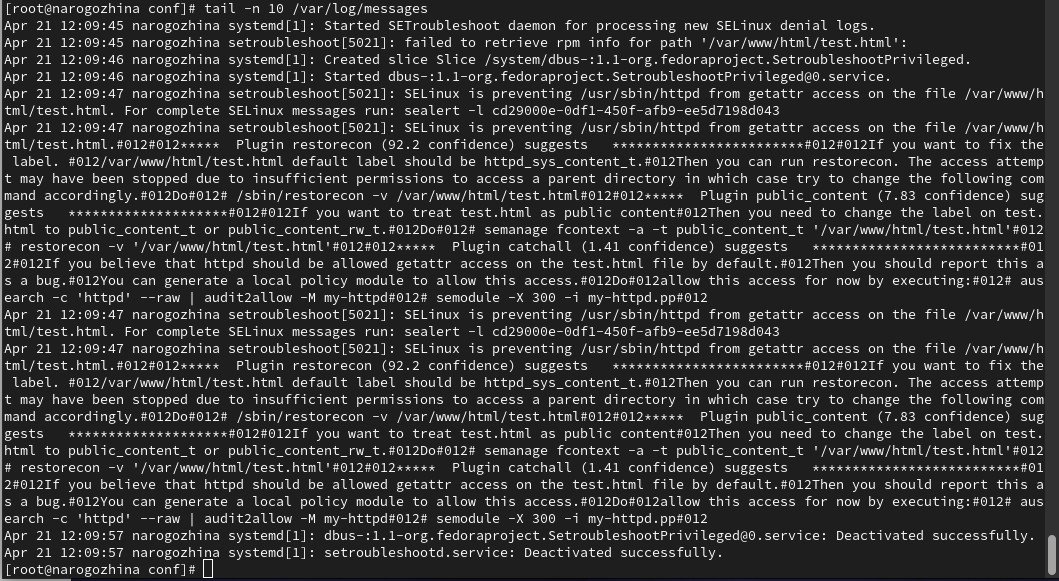
попытка №1

1. ls -l /var/www/html/test.html (рис. [??]).

выполнение команды

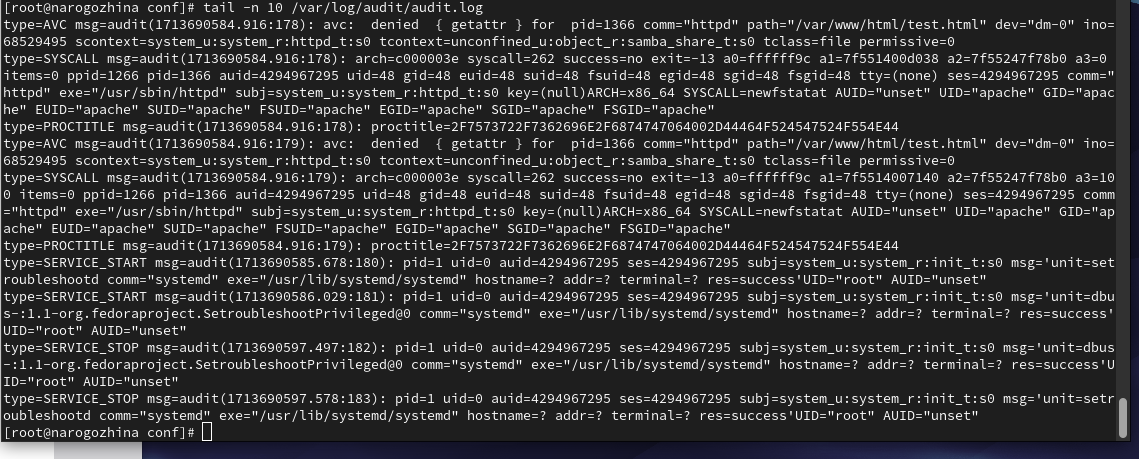
выполнение команды

Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл (рис. [??]).



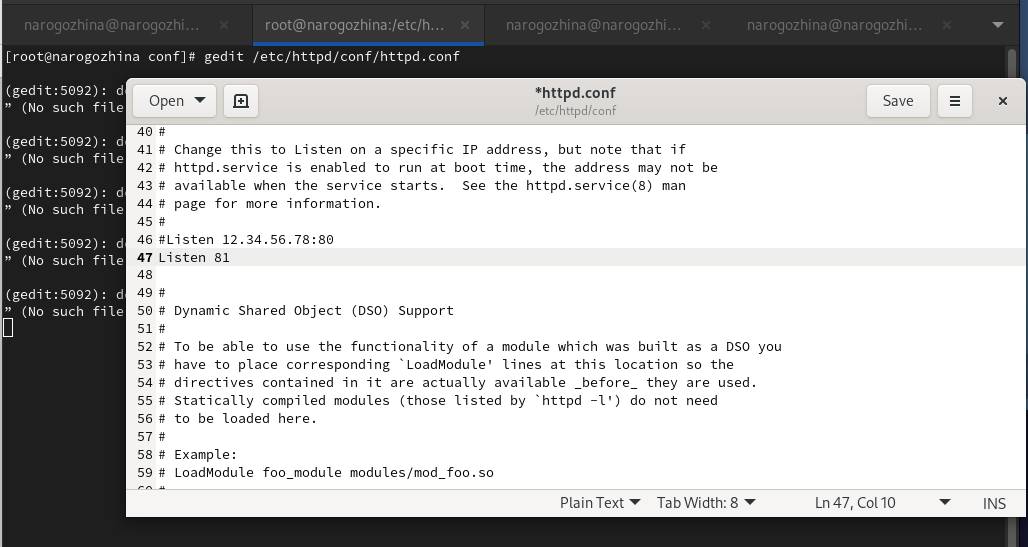
Системный лог-файл

Если в системе окажутся запущенными процессы setroubleshootd и audtd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log. Проверьте это утверждение самостоятельно (рис. [??]).



audit.log

1. 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. [??]).



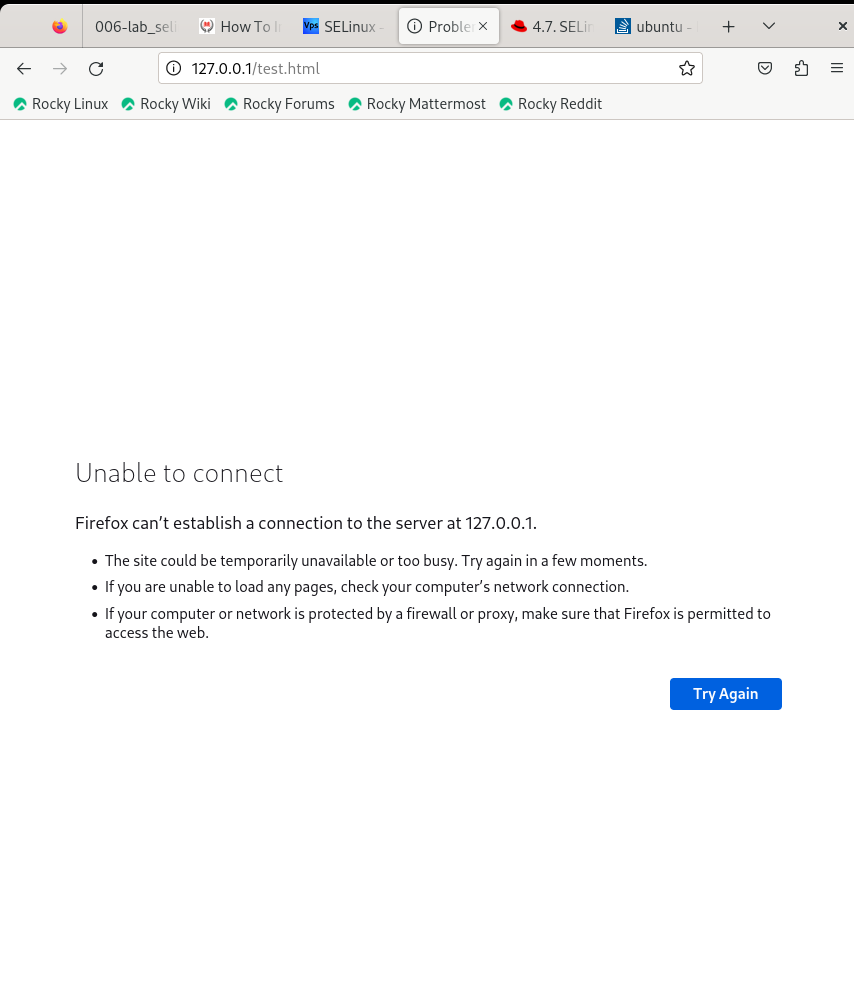
Listen 80 -> Listen 81

1. Выполните перезапуск веб-сервера Apache (рис. [??]).

restart

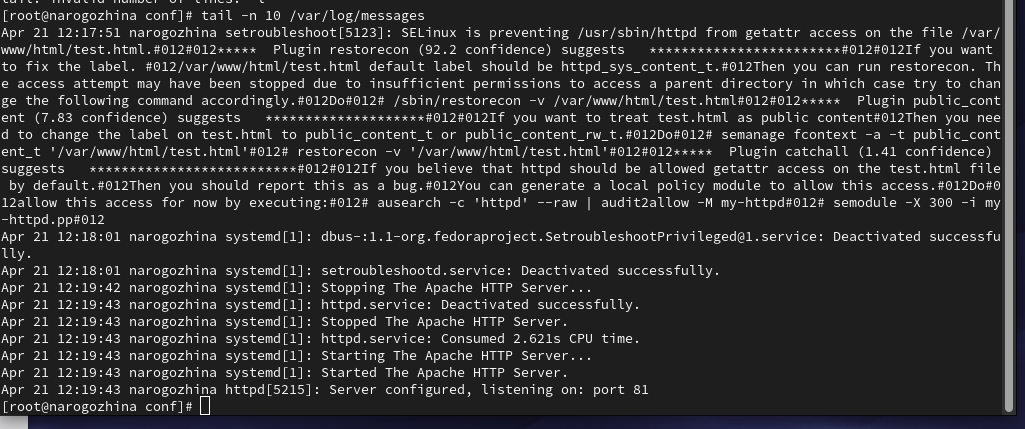
restart

При попытке переподключиться - произошел сбой, т.к. мы подключаемся по другому tcp серверу (рис. [??]).



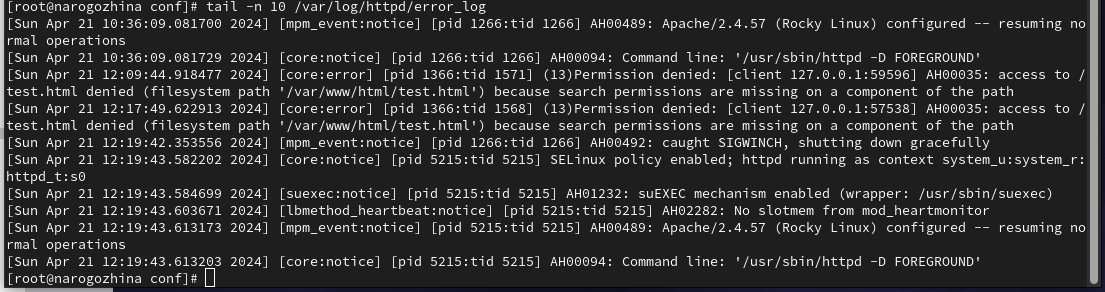
Попытка №2

1. Проанализируйте лог-файлы: tail -nl /var/log/messages(рис. [??]).

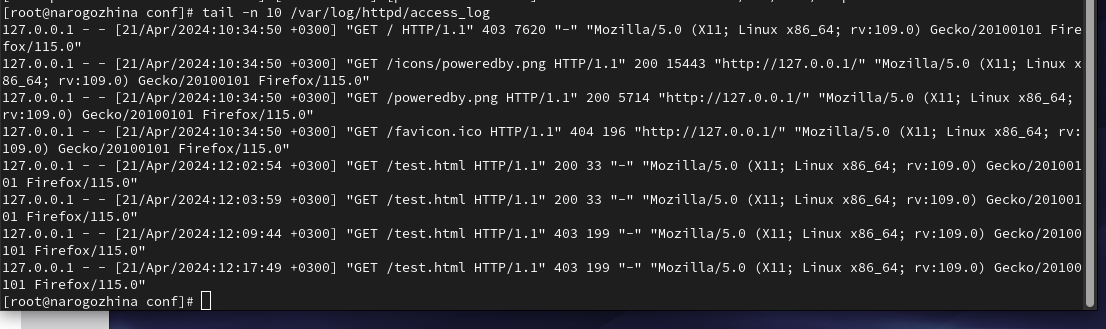


tail -nl /var/log/messages

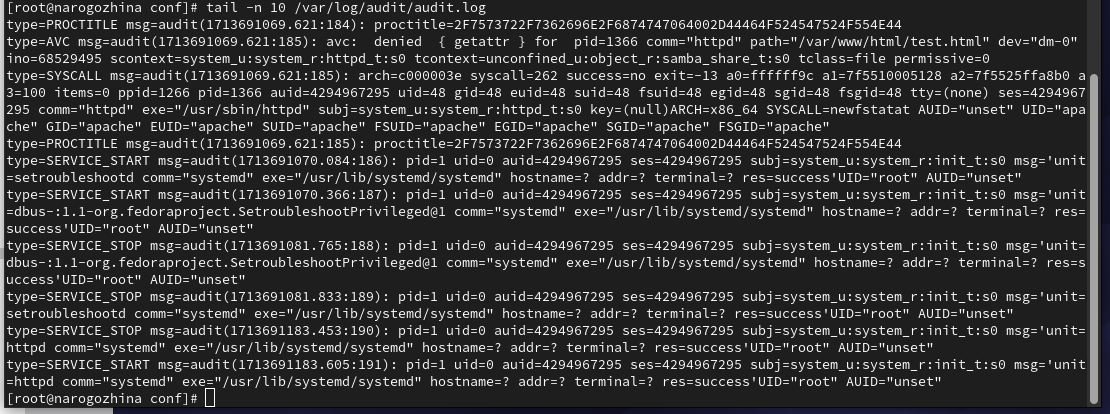
Просмотрите файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log и выясните, в каких файлах появились записи (рис. [??], рис. [??], рис. [??]).



/var/log/http/error\_log

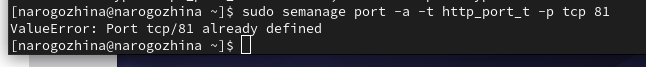


/var/log/http/access\_log



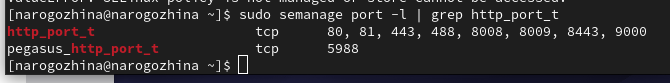
var/log/audit/audit.log

1. Выполните команду semanage port -a -t http\_port\_t -р tcp 81 (рис. [??]).



semanage

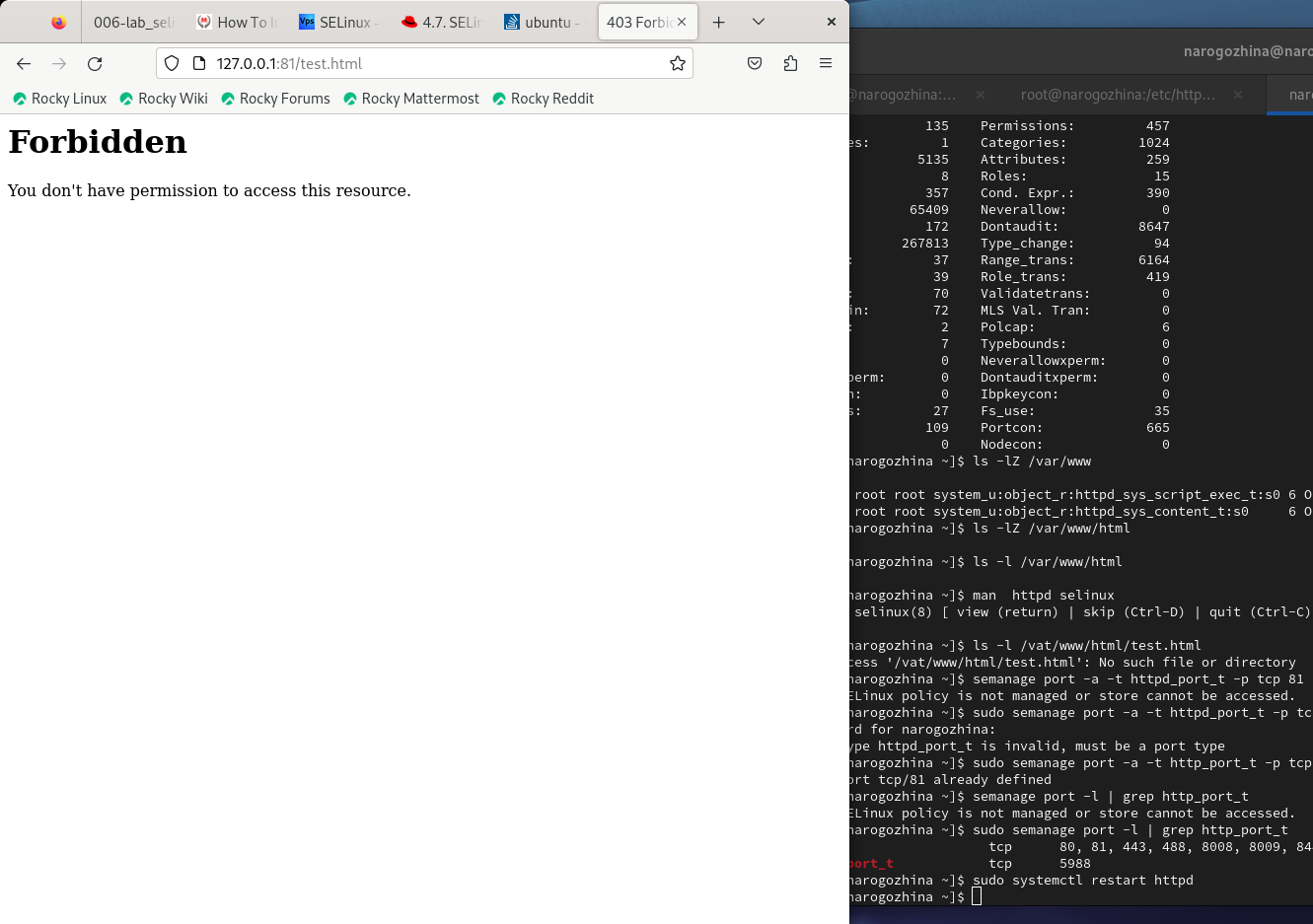
После этого проверьте список портов командой semanage port -l | grep http\_port\_t (рис. [??]).



semanage grep

Порт 81 появился в списке.

1. Попробуйте запустить веб-сервер Apache ещё раз (рис. [??]).



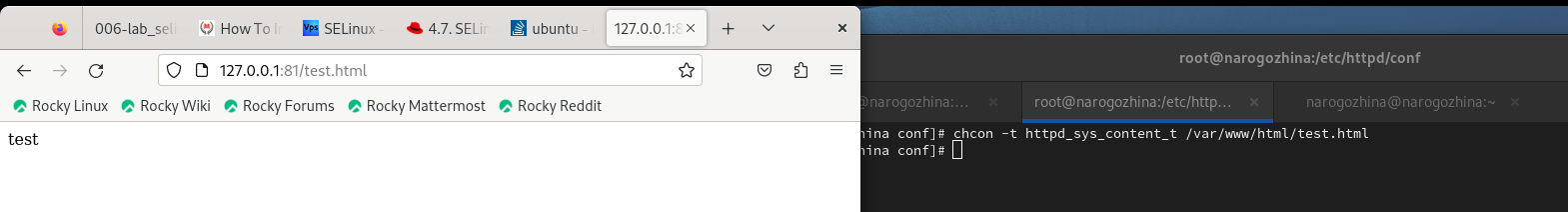
Попытка №3

Сейчас мы подключаемся к серверу, который знаком нашей программе, и поэтому подключение у нас прошло. Да, доступа у нас нет, но тем не менее, сервер запустился, а не выдал ошибку.

1. Верните контекст httpd\_sys\_cоntent\_\_t к файлу /var/www/html/ test.html:

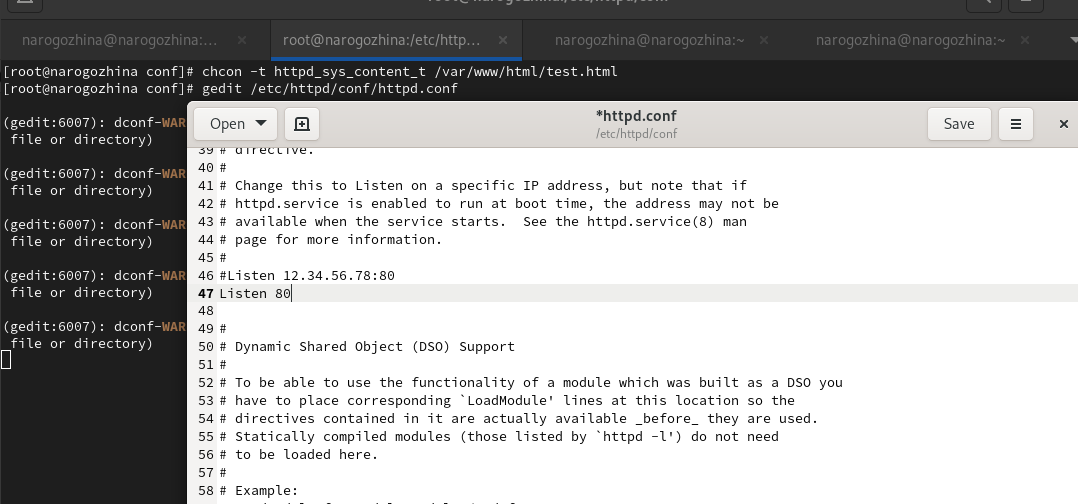
chcon -t httpd\_sys\_content\_t /var/www/html/test.html

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. [??]).



test.ru

1. Исправьте обратно конфигурационный файл apache, вернув Listen 80 (рис. [??]).

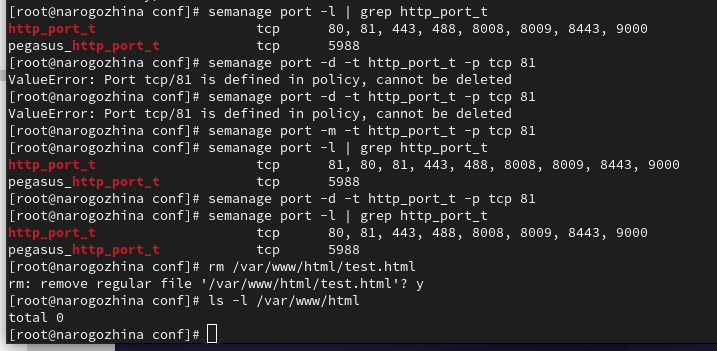


change back

1. Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и проверьте, что порт 81 удалён.
2. Удалите файл /var/www/html/test.html:

rm /var/www/html/test.html

(рис. [??]).



rm test.html

# 4 Выводы

В ходе лабораторной работы мы развили навыки администрирования ОС Linux, получить первое практическое знакомство с технологией SELinux1, а также проверили работу SELinx на практике совместно с веб-сервером Apache.

# Список литературы