Отчёт

по лабораторной работе 6

Агеева Анастасия Борисовна

Содержание

# Цель работы

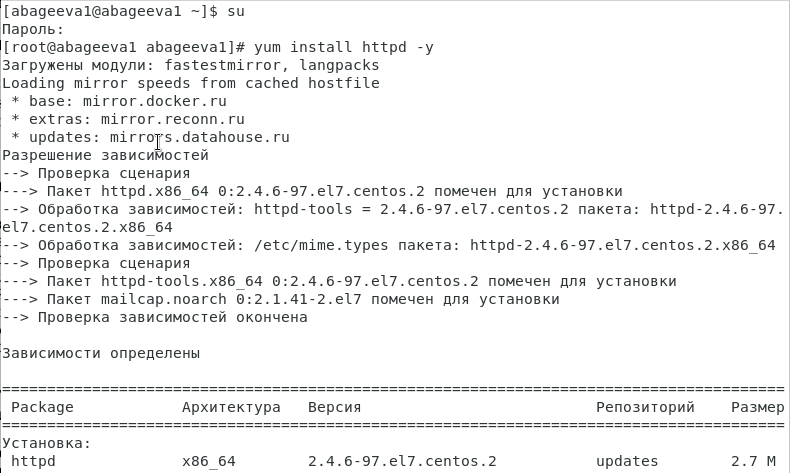
Развить навыки администрирования ОС Linux. Получить первое прак- тическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Задание

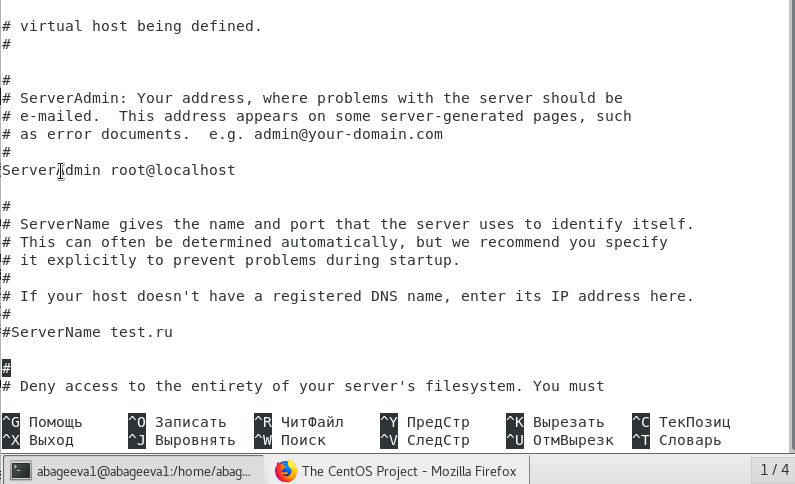
Лабораторная работа подразумевает использование стандартного дистрибутива Linux CentOS с включённой политикой SELinux targeted и режимом enforcing

# Выполнение лабораторной работы

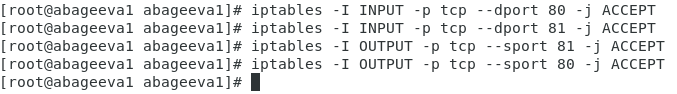
1. Установим/обновим веб-сервер Apache (рис.1).

* 
* Figure 1: рис.1. Обновление Apache.

1. В конфигурационном файле /etc/httpd/conf/httpd.conf зададим параметр ServerName (рис.2).

* 
* Figure 2: рис.2.

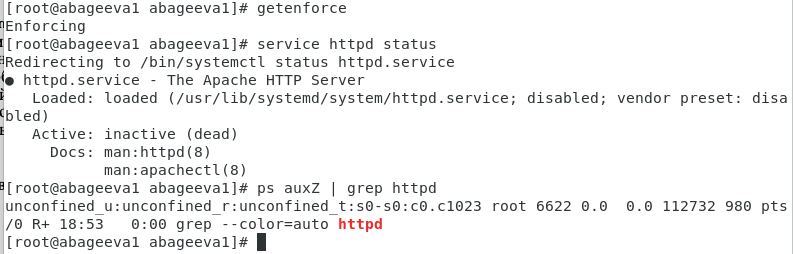
1. Добавим разрещающие правила для подключения к 80-у и 81-у портам протокола TCP (рис.3-6).

* 
* Figure 3: рис.3

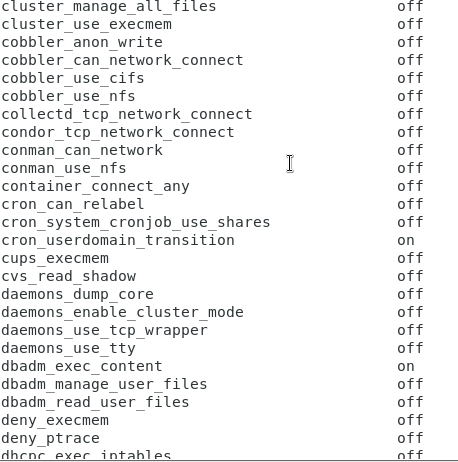
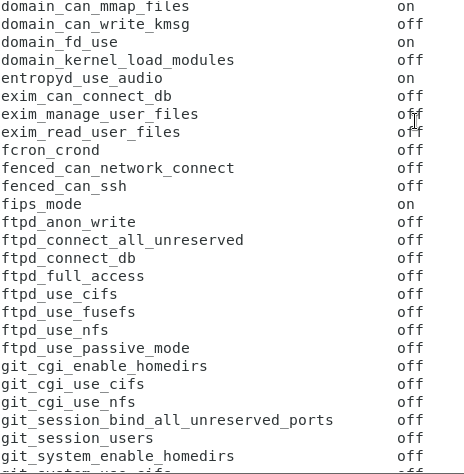
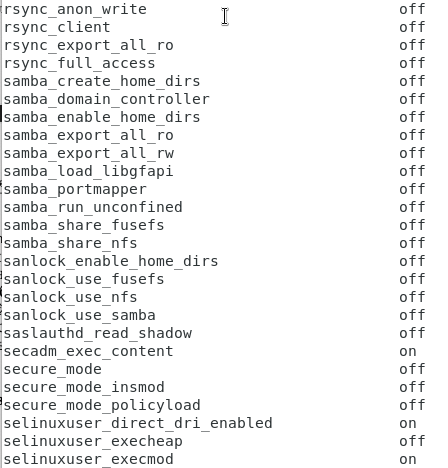
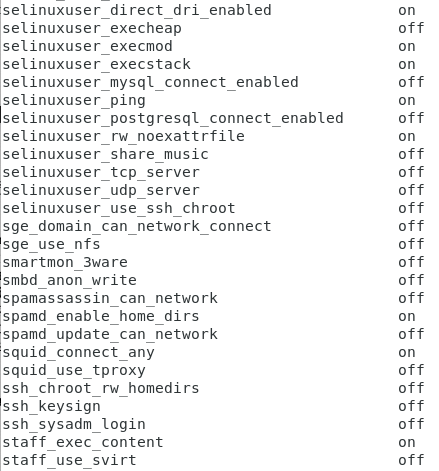
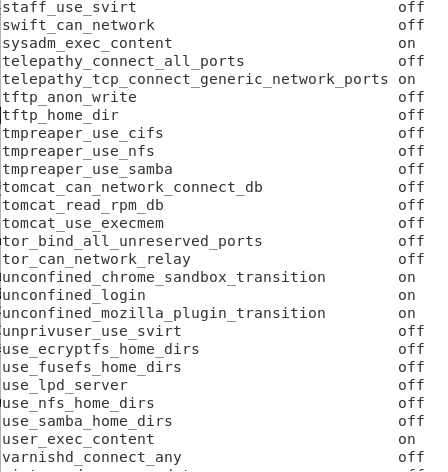
1. Убедимся, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus (Рис. 4)
2. Обратимся к веб-серверу, запущенному на нашем стенде, и убедимся, что он работает. (рис.4).

* 
* Figure 4: рис.4

1. Найдем Apache в списке процессов, определим его контекст безопасности. В нашем случае контекст безопасности unconfined\_u:system\_r:httpd\_t (Рис. 5)

* 
* Figure 5: рис.5

1. Посмотрим текущее состояние переключателей SELinux для Apache. Многие из переключателей в положении “off” (рис.6-14).

* 
* Figure 6: рис.6
* 
* Figure 7: рис.7
* 
* Figure 8: рис.8
* 
* Figure 9: рис.9
* 
* Figure 10: рис.10
* 
* Figure 11: рис.11
* 
* Figure 12: рис.12
* 
* Figure 13: рис.13
* 
* Figure 14: рис.14

1. Посмотрим статистику по политике с помощью команды seinfo, также определим множество пользователей, ролей и типов. Пользователей: 9 Ролей: 12 Типов: 3920 (рис.15).
2. Определим тип файлов и поддиректории, находящихся в директории /var/www (рис.15).
3. Определим тип файлов, находящихся в директории /var/www/html (рис.15).

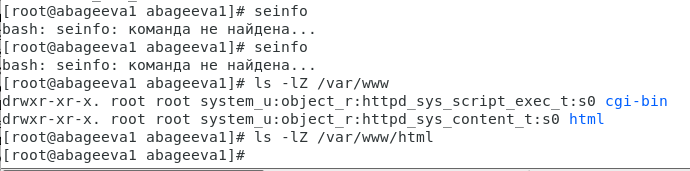


Figure 15: рис.15

1. Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html (рис.17).

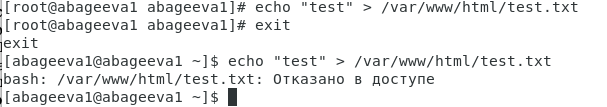


Figure 16: рис.17

1. По рисунку видно, что только root может создать файл в данной директории.
2. В следствие этого создадим от имени суперпользователя html-файл /var/www/html/test.html следующего содержания (рис.18).



Figure 17: рис.18

1. Проверим контекст созданного файла. В нашем случае контекст unconfined\_u:object\_r:httpd\_sys\_content\_t (рис.19).

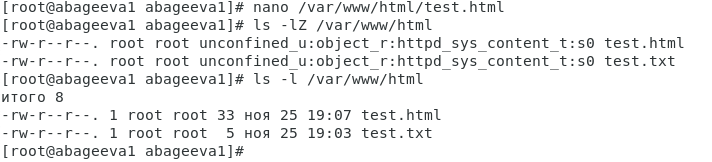


Figure 18: рис.19

1. Обратимся к файлу через веб-сервер, введя в firefox адрес http://127.0.0.1/test.html Убедимся, что файл был успешно отображен (рис.20).



Figure 19: рис.20

1. Проверим контекст файла. Т.к. по умолчанию пользователи CentOS являются unconfined от типа, созданному нами файлу test.html был сопоставлен SELinux, пользователь unconfined\_u. Это первая часть контекста. Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль object\_r используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. Тип httpd\_sys\_content\_t позволяет процессу httpd получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер. (рис.21).
2. Изменим контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_shate\_t. Как видно из рисунка, контекст успешно сменился. (рис.21).



Figure 20: рис.21

1. Попробуем еще раз получить доступ к файлу через веб-сервер, введя в firefox адрес http://127.0.0.1/test.html. Как видно из рисунка, мы получили сообщение об ошибке. (рис.22).

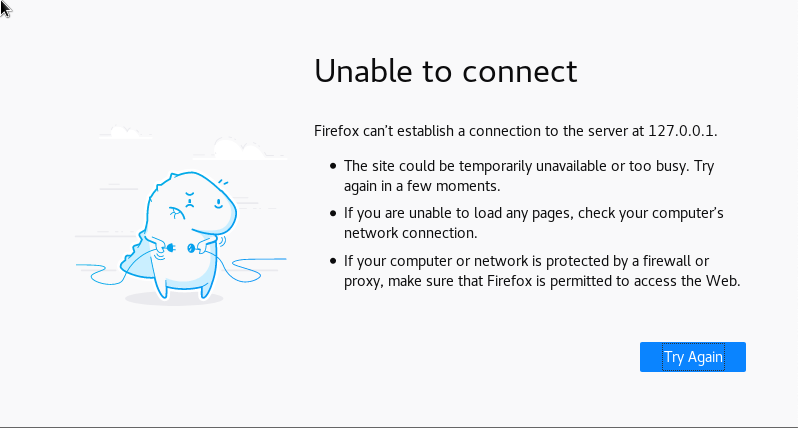


Figure 21: рис.22

1. Проанализируем ситуацию, просмотрев log-файлы веб-сервера Apache, системный log-файл и audit.log при условии уже запущенных процессов setroubleshootd и audtd. Исходя из log-файлов, мы можем заметить, что проблема в измененном контексте на шаге 17, т.к. процесс httpd не имеет доступа на samba\_share\_t. (рис.23-25).

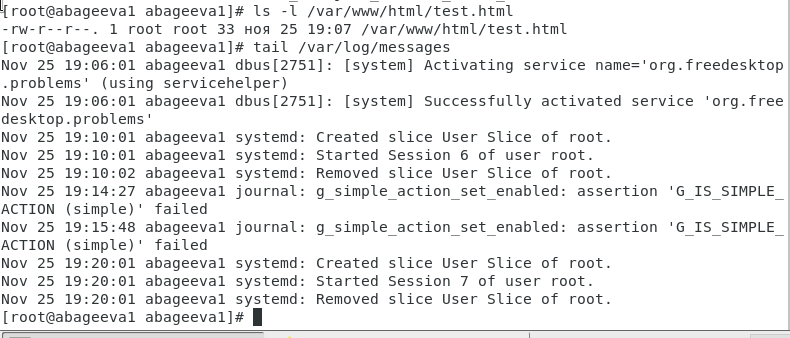


Figure 22: рис.23



Figure 23: рис.24

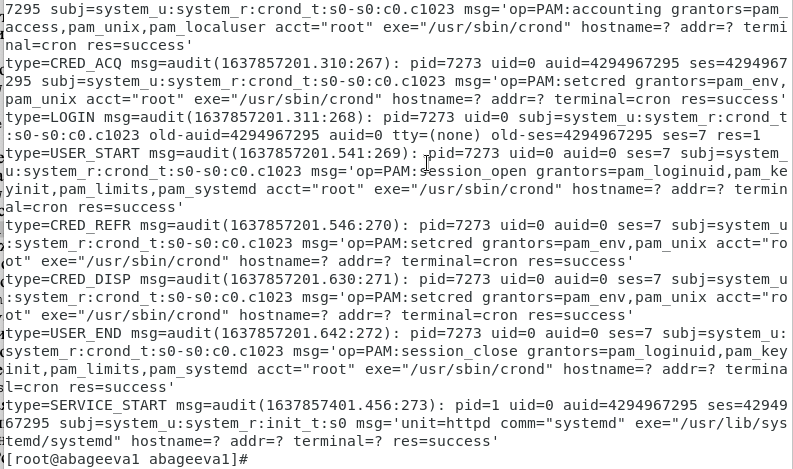


Figure 24: рис.25

1. Попробуем запустить Apache на прослушивание TCP-порта 81, заменив в файле /etc/httpd/conf/httpd.conf строчку Listen 80 на Listen 81. (рис.26).

Figure 25: рис.26

Figure 25: рис.26

1. Перезапустим Apache и попробуем обратиться к файлу через веб-сервер, введя в firefox адрес http://127.0.0.1/test.html. Из этого можно сделать предположение, что в списках портов, работающих с веб-сервером Apache, отсутствует порт 81. (рис.27-28).

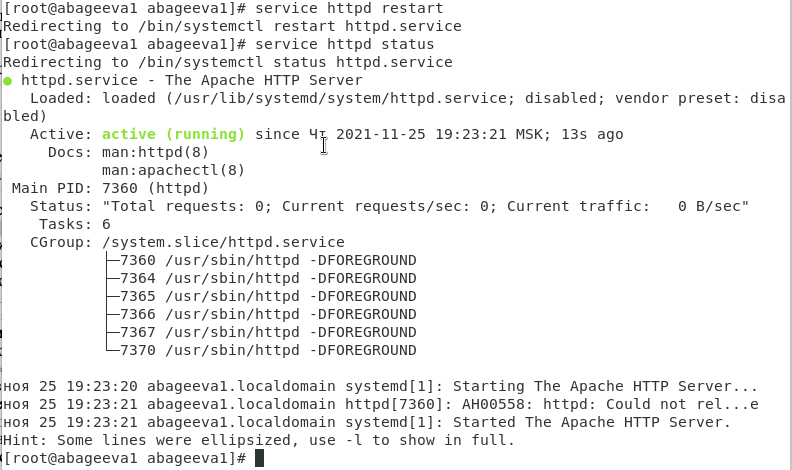


Figure 26: рис.27

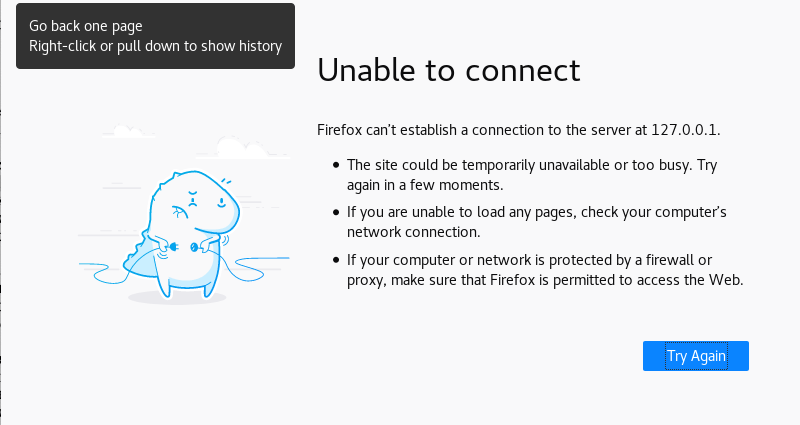


Figure 27: рис.28

1. Подтвердим свои догадки, просмотрев log-файлы. Во всех log-файлах появились записи, кроме /var/log/messages. (рис.29).

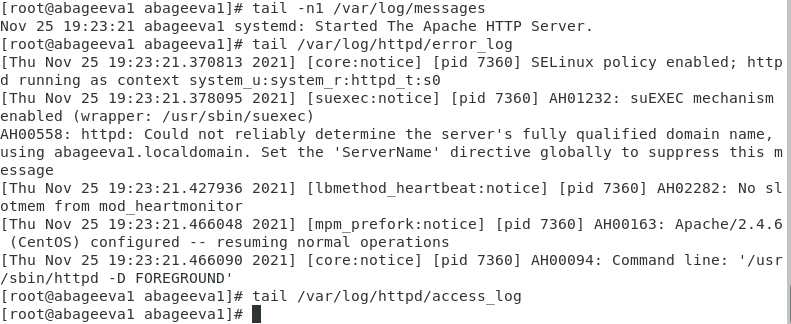


Figure 28: рис.29

1. Чтобы подключиться к веб-серверу через порт 81, добавим его с помощью команды semanage port –a –t http\_port\_t –p tcp 81 После этого проверим список портов semanage port –l | grep http\_port\_t. (рис.32).

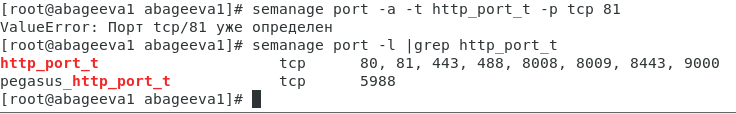


Figure 29: рис.32

1. Попробуем теперь запустить веб-сервер еще раз. Добавив порт 81 в систему, Apache cмог прослушать данный порт, в следствие чего получилось обратиться к файлу test.html. (рис.33-34).

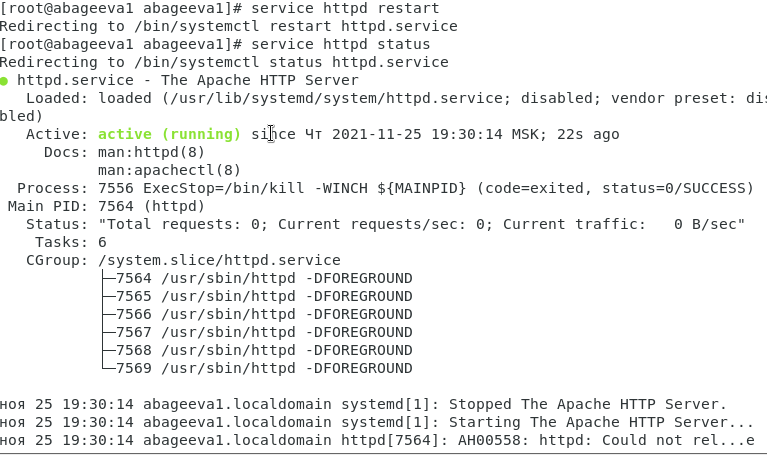


Figure 30: рис.33

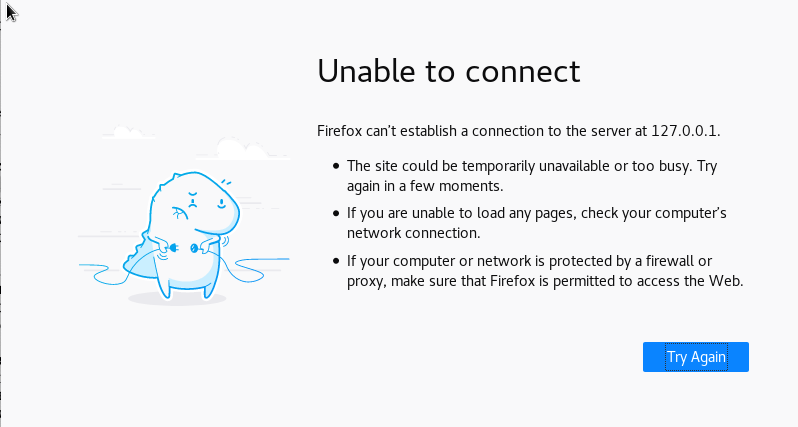


Figure 31: рис.34

1. Вернем обратно контекст httpd\_sys\_content\_t к файлу /var/www/html/test.html. После этого вновь попробуем получить доступ к файлу через веб-сервер, введя в firefox адрес http://127.0.0.1:81/test.html. (рис.35-36).

Figure 32: рис.35

Figure 32: рис.35

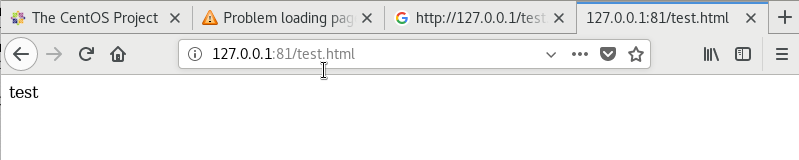


Figure 33: рис.36

1. Исправим обратно конфигурационный файл Apache, вернув Listen 80 (рис.37).

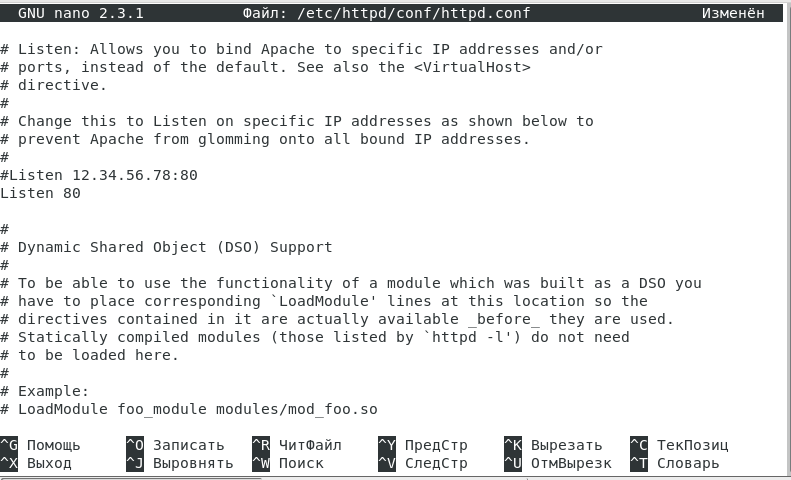


Figure 34: рис.37

1. Удалим привязку http\_port\_t к 81 порту (рис.38).
2. Проверим, что порт 81 удален. (рис.38).
3. Удалим файл /var/www/html/test.html (рис.38).

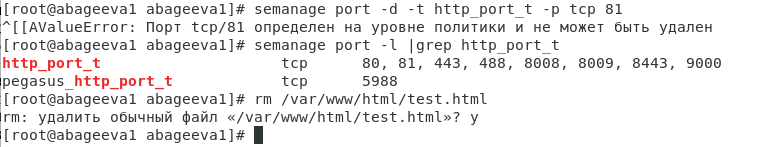


Figure 35: рис.38

# Выводы

Я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux, а также проверила работу SELinx на практике совместно с веб-сервером Apache.