Лабораторная работа No 6.

Сагдеров Камал, НФИбд-04-22

Содержание

# 1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux.

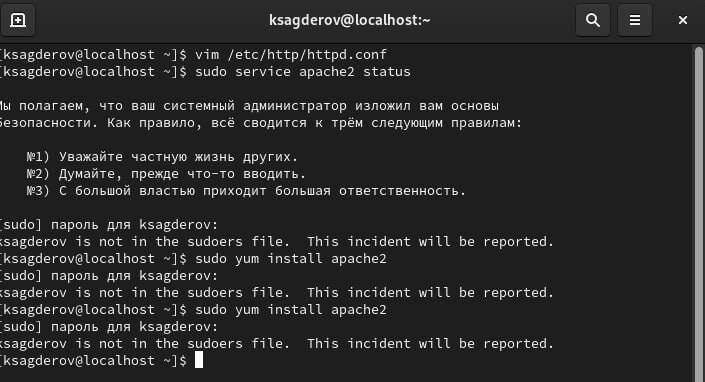
# 2 Выполнение лабораторной работы

## 2.1 Подготовка лабораторного стенда

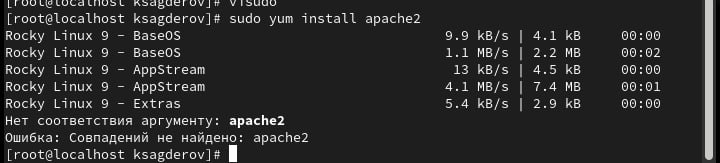
1. Установить Apache2 при помощи dnf.

dnf install httpd

1. В конфигурационном файле httpd.conf прописать параметр ServerName (??).

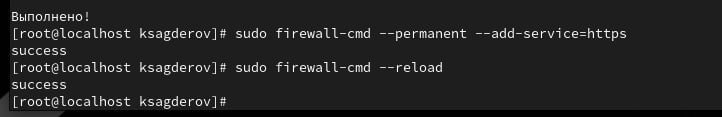


ServerName



ServerName

1. Отключить пакетный фильтр при помощи iptables (??).



iptables

[ServerName](./image/4.png)

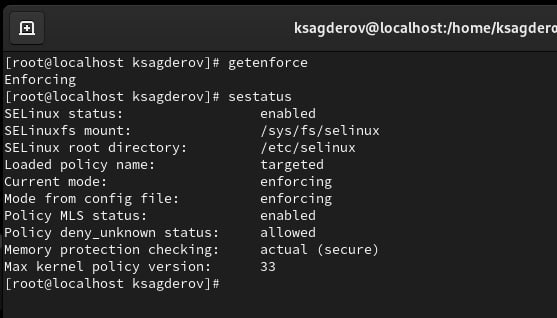
[ServerName](./image/5.png)

[ServerName](./image/6.png)

[ServerName](./image/15.png)

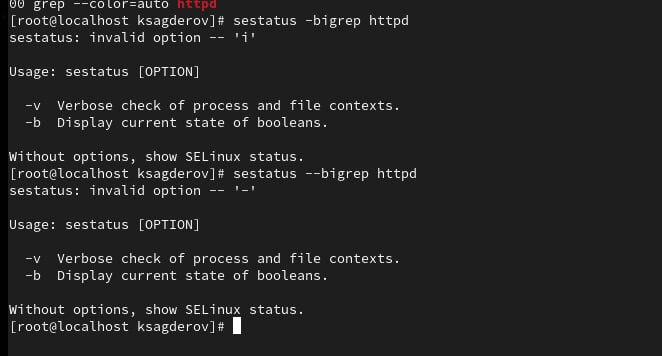
## 2.2 Выполнение

1. Проверим правильность работы SELinux. Должен быть выставлен режим enforcing политики targeted (??).



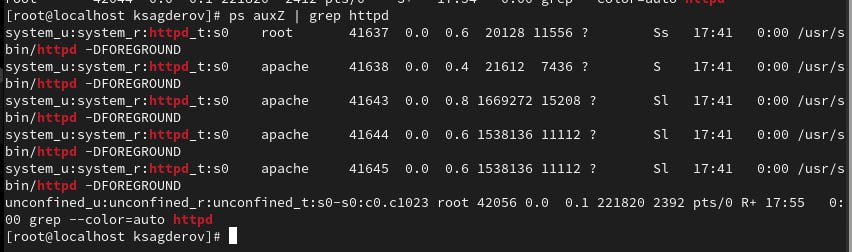
sestatus

1. Запустим Apache веб-сервер (??).



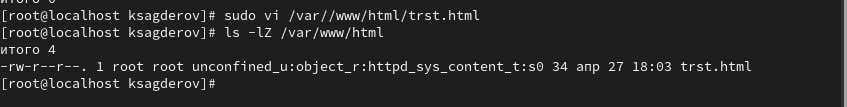
httpd

1. В списке процессов найдем httpd (??). На этот процесс выставлен следующий контекст безопасности (первый столбец изображения [**gentooSELinuxTutorialsLinuxServices?**]).



Контекст безопасности

1. Посмотрим текущее состояние переключателей SELinux для Apache2 (??).
2. Также посмотрим текущую статистику по политике (??).



Статистика по политике

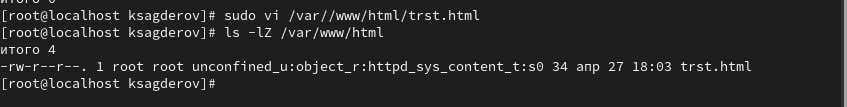
1. Посмотрим текущий контекст безопасности для файлов и поддиректорий в директории /var/www (??).

* Установлен контекст httpd\_sys\_script\_exec\_t для cgi-скриптов, чтобы был разрешен им доступ ко всем sys-типам.
* Установлен контекст httpd\_sys\_content\_t для содержимого, которое должно быть доступно для всех скриптов httpd и для самого демона.

|  |
| --- |
| Статистика по политике |

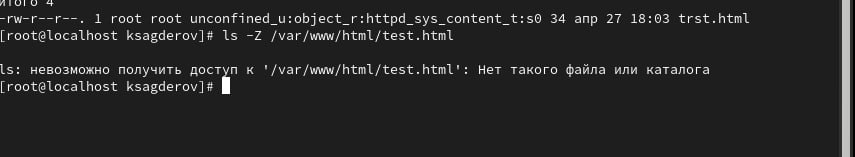
Статистика по политике

1. В директории /var/www/html пусто.



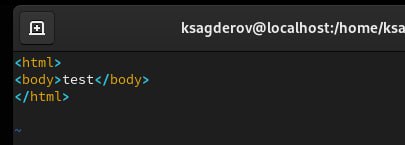
/var/www/html

1. В директории /var/www/html создавать папки может только root (право w есть только у него).



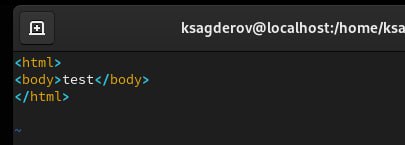
Статистика по политике

1. Создадим файл /var/www/html/test.html (??).



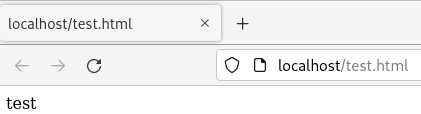
test.html

1. Проверим контекст созданного нами файла (??).



test.html

1. Перейдем в браузер и в нем проверим доступность данного файла (??).



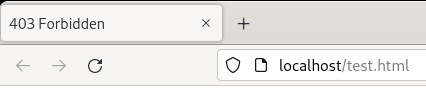
Проверка

1. Изменим конекст файла, чтобы Apache не смог получить доступ (??).

test.html

test.html

1. Проверим, что доступ к файлу стал не доступен (??).



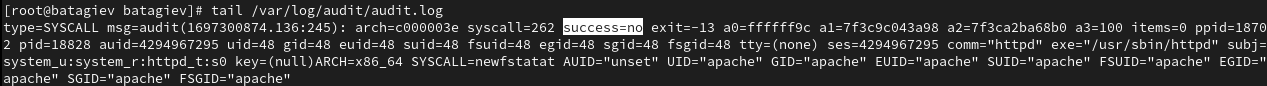
Проверка

1. Посмотрим логи от веб-сервера Apache (??).

/var/log/messages

/var/log/messages

Также проверим audit.log (??).



/var/log/audit/audit.log

1. Поменяем порт, на котором работает Apache.

Порт 81

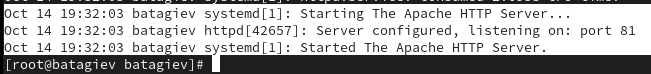
Порт 81

1. Перезапустим веб-сервер (успешно).

Перезапуск

Перезапуск

1. В логах наблюдаем запуск сервера на 81 порту.



/var/log/messages

1. Добавим порт в semanage для http\_port\_t и проверим его добавление

Добавление

Добавление

Проверка

Проверка

1. Ввернем контекст файлу test.html.
2. Удалим привязку порта.
3. Удалим файл test.html.

# 3 Выводы

В результате выполнения работы я выполнил цели работы.