Лабораторная работа №6

Дисциплина: Основы информационной безопасности

Коновалова Татьяна Борисовна

Содержание

# 1 Цель работы

Цель лабораторной работы — Получить практические навыки адмирирования в OC Linux и ознакомиться с технологией SELinux совместно с веб-сервером Apache.

# 2 Теоретические данные

SELinux, или Security Enhanced Linux, — это продвинутый механизм управления доступом, разработанный Агентством национальной безопасности (АНБ) США для предотвращения злонамеренных вторжений. Он реализует мандатную модель управления доступом (MAC — Mandatory Access control) в дополнение к уже существующей в Linux дискреционной модели (DAC — Discretionary Access Control), то есть разрешениям на чтение, запись, выполнение.

У SELinux есть три режима работы:

* Enforcing — ограничение доступа в соответствии с политикой. Запрещено все, что не разрешено в явном виде. Режим по умолчанию.
* Permissive — ведёт лог действий, нарушающих политику, которые в режиме enforcing были бы запрещены, но не запрещает сами действия.
* Disabled — полное отключение SELinux.

В основе структуры безопасности SELinux лежат политики. Политика — это набор правил, определяющих ограничения и права доступа для всего, что есть в системе. Под “всем” в данном случае понимаются пользователи, роли, процессы и файлы. Политика определяет связь этих категорий друг с другом. |

Apache — это свободное программное обеспечение, с помощью которого можно создать веб-сервер. Несмотря на то, что Apache чаще всего называют сервером (более того, его официальное название — Apache HTTP Server) — это всё-таки программа, которую устанавливают на сервер, чтобы добиться определённых результатов.

Для чего нужен Apache сервер:

* чтобы открывать динамические PHP-страницы,
* для распределения поступающей на сервер нагрузки,
* для обеспечения отказоустойчивости сервера,
* чтобы потренироваться в настройке сервера и запуске PHP-скриптов.

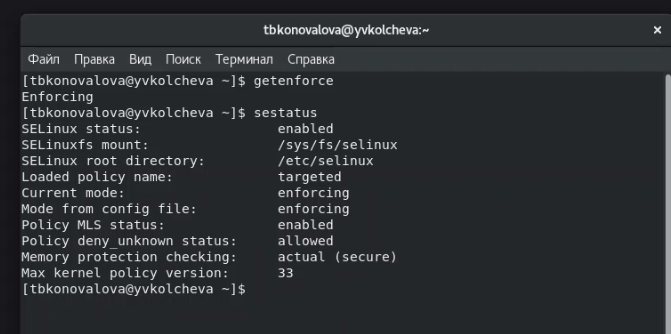
Apache является кроссплатформенным ПО и поддерживает такие операционные системы, как Linux, BSD, MacOS, Microsoft, BeOS и другие.

# 3 Задание

1.Найти веб-сервер Apache в списке процессов, определить его контекст безопасности и занести эту информацию в отчёт. 2.Посмотреть текущее состояние переключателей SELinux для Apache; 3.Изучить справку man httpd\_selinux 4.Определить тип файлов, находящихся в директории /var/www/htm.

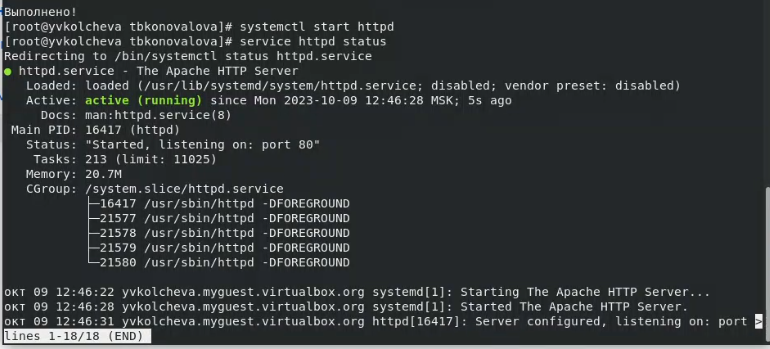
# 4 Выполнение лабораторной работы

1.Вошла в систему под своей учетной записью и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команды getenforce и sestatus (рис. [??]).



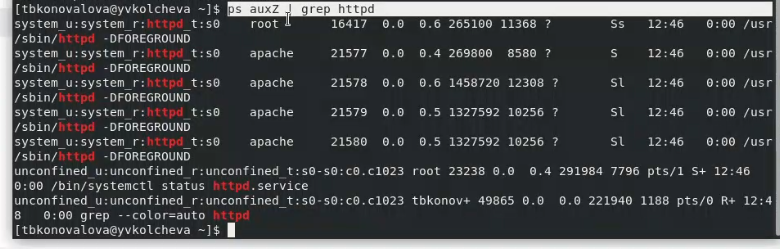
getenforce и sestatus

2.Убедилась, что сервер работает с помощью команды service httpd status (рис. [??]).



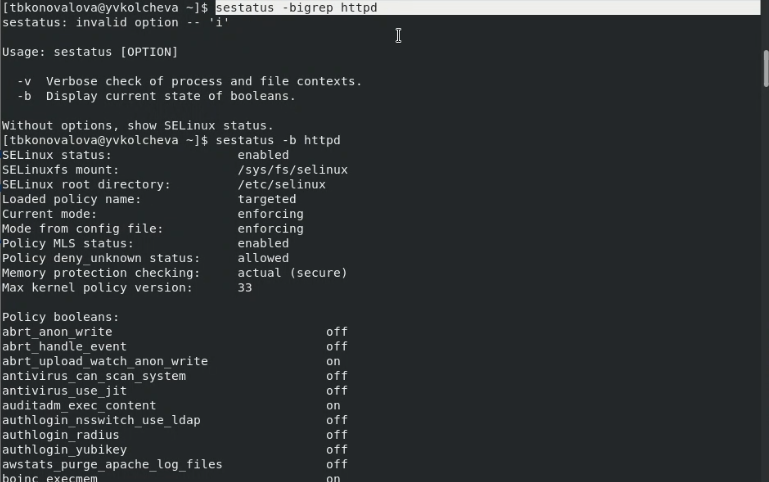
Проверка работы сервера

3.С помощью команды ps -eZ нашла, что контекст безопасности Apache — httpd\_t (рис. [??]).



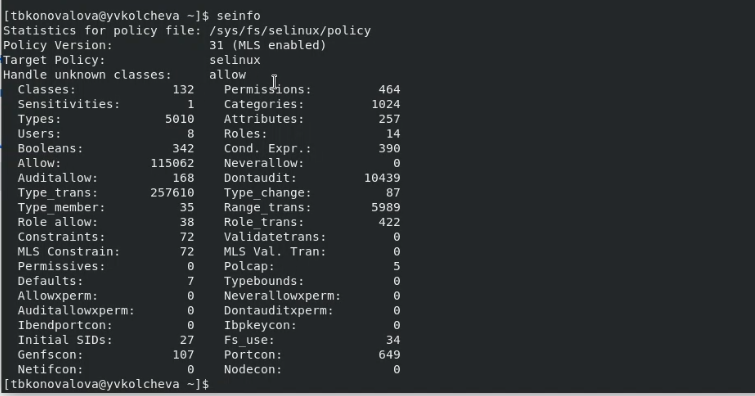
Контекст безопасности Apache

4.Посмотрела текущее состояние переключателей командой sestatus -b httpd (рис. [??]).



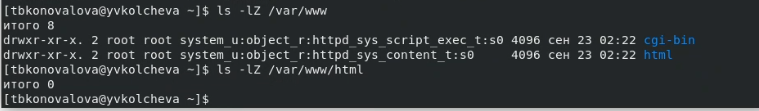
Состояние переключателей

5.Посмотрела статистику по политике командой seinfo. Узнала, что множество пользователей — 8, ролей — 14, типов — 5010 (рис. [??]).



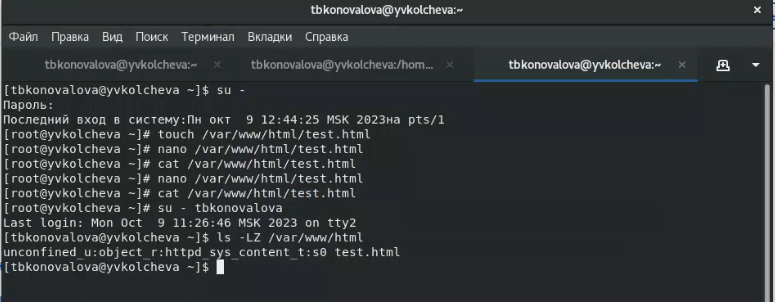
Статистика seinfo

6.Определила тип файлов и круг пользователей с правой на создание и поддиректорий в директориях /var/www и /var/www/html командой ls -lZ (рис. [??]).



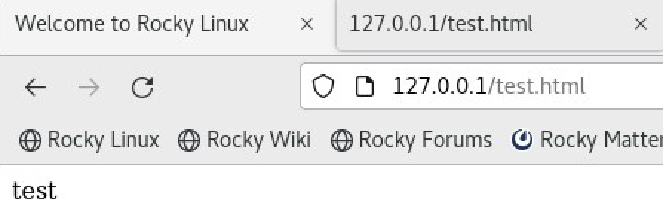
Данные директорий /var/www и /var/www/html

7.От имени суперпользователя создала файл /var/www/html/test.html (рис. [??]).



Файл test.html

Обратилась к файлу через веб-сервер, введя в браузер адрес “http://127.0.0.1/test.html”. Файл был успешно отображен (риc. [-#fig:008]).



Обращение к файлу через веб-сервер

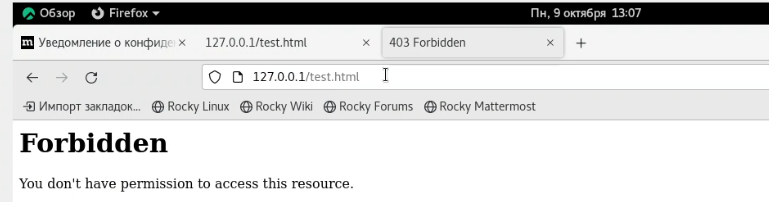
8.Изучив справку man httpd\_selinux, выяснила, что для httpd определены следующие контексты файлов: httpd\_sys\_content\_t, httpd\_sys\_script\_exec\_t, httpd\_sys\_script\_ro\_t, httpd\_sys\_script\_rw\_t, httpd\_sys\_script\_ra\_t, httpd\_unconfined\_script\_exec\_t.

Контекст моего файла - httpd\_sys\_content\_t (в таком случае содержимое должно быть доступно для всех скриптов httpd и для самого демона). Изменила контекст файла на samba\_share\_t командой “sudo chcon -t samba\_share\_t /var/www/html/test.html” . После этого убедилась, что контекст поменялся (риc. [-#fig:009]).



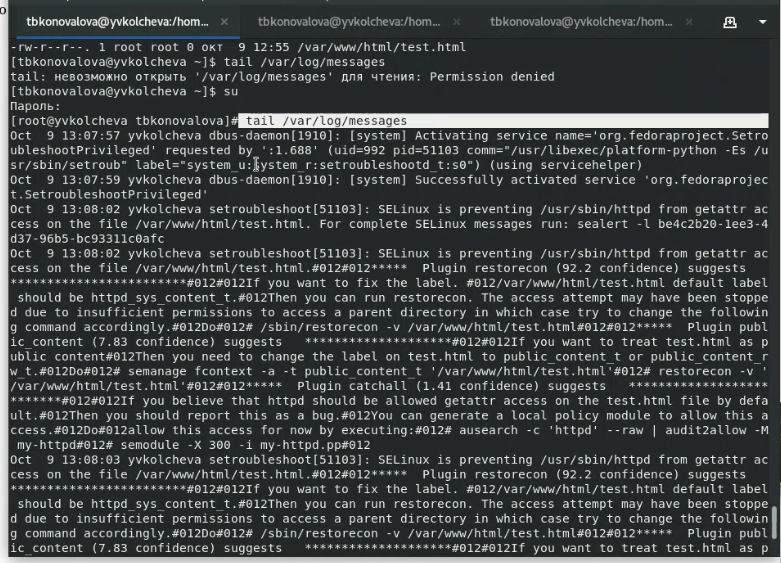
Изменение контекста файла

9.При повторной попытке открыть файл через веб-браузер я получила ошибку доступа (рис. [??]).



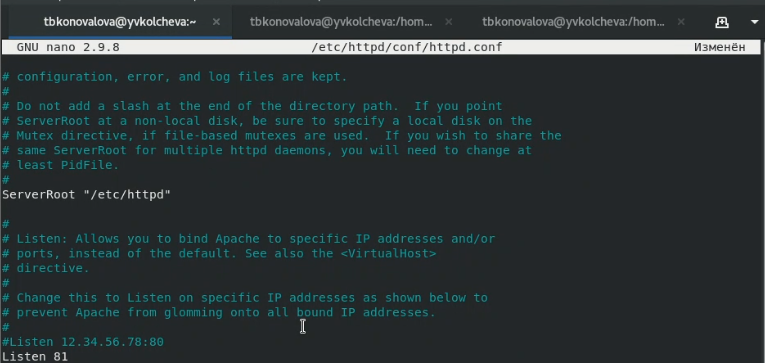
Ошибка доступа при открытии файла через веб-сервер

10.Убедилась, что файл доступен для чтения всем пользователям командой ls -l. Далее посмотрела log-файлы веб-сервера Apache командой tail, где показаны ошибки (рис. [??]).



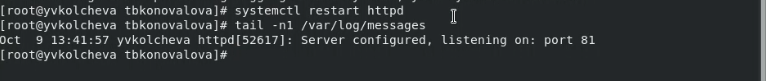
Ошибки в log-файлах

11.Устновила веб-сервер Apache на прослушивание TCP-порта 81, изменяя строку Listen в файле /etc/httpd/conf/httpd.conf (рис. [??]).



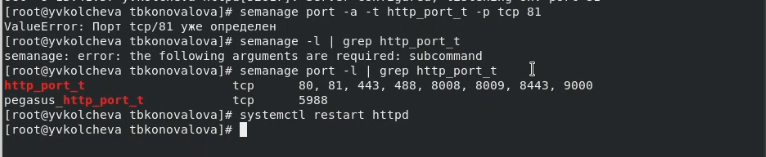
Прослушивание 81 порта

12.Перезапустила сервер и увидела данные log-файлов веб-сервера Apache (рис. [??]).



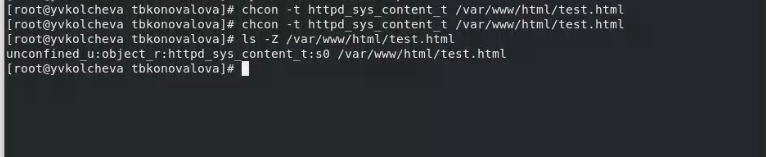
Перезапуск сервера

13.Устновила для веб-сервера Apache порт TCP-81 и проверила его наличие в списке портов командой semanage (рис. [??]).

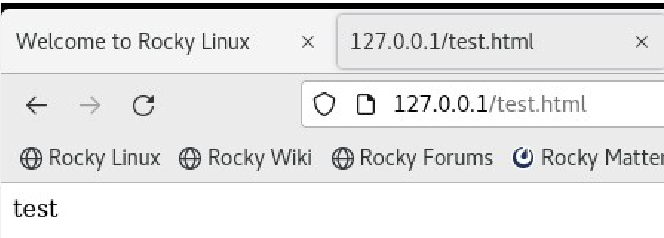


Установка порта

14.Вернула файлу test.html контекст httpd\_sys\_content\_t и снова успешно просмотрела страницу в веб-браузере (рис. [??]) и (рис. [??]).

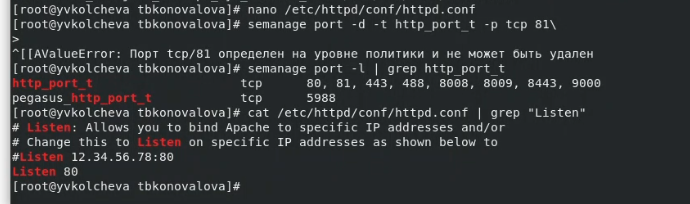


Возвращаем файлу исходный контекст



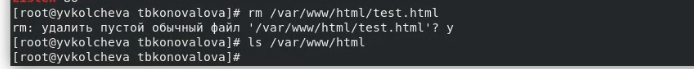
Повторный просмотр файла в веб-браузере

17.Вернула в конфигурационный файл прослушивание порта 80 и удалила порт 81 из списка портов (рис. [??]).



Удаление порта

18.Удалила файл test.html (рис. [??]).



Удаление файла

# 5 Выводы

Получила практические навыки адмирирования в OC Linux и ознакомилась с технологией SELinux совместно с веб-сервером Apache.

# 6 Библиография

СПИСОК ЛИТЕРАТУРЫ

1.Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: http://bugtraq.ru/library/books/attack1/index.html

2.Теоеретические знания, приведённые в Лабораторной работе №6 - https://esystem.rudn.ru/pluginfile.php/2090131/mod\_resource/content/2/006-lab\_selinux.pdf

3.Запечников С. В. и др. Информационн~пасность открытых систем. Том 1. — М.: Горячаая линия -Телеком, 2006.

СПИСОК ИНТЕРНЕТ-ИСТОЧНИКОВ

1.[Электронный ресурс] - доступ: https://codeby.school/blog/informacionnaya-bezopasnost/razgranichenie-dostupa-v-linux-znakomstvo-s-astra-linux

2.[Электронный ресурс] - доступ: https://debianinstall.ru/diskretsionnoe-razgranichenie-dostupa-linux/