Лабораторная работа №6

Мандатное разграничение прав в Linux

Дмитрий Константинович Федотов

Содержание

1 Цель работы **5**

2 Задание **6**

3 Выполнение лабораторной работы **7**

4 Выводы **15**

5 Список литературы **16**

Список иллюстраций

3.1 Установка Apache 7
3.2 Внемение информации в конфигурационный файл 7
3.3 Отключение пакетного фильтра 8
3.4 Проверка режима работы SELinux 8
3.5 Проверка работы веб-сервера 8
3.6 Поиск веб-сервера Apache и определение его контекста безопасности 9
3.7 Ттекущее состояние переключателей SELinux для Apache 9
3.8 Статистика по политике 10
3.9 Определение типов файлов и поддиректорий, находящихся в директории `/var/www` 10
3.10 Определение типов файлов и поддиректорий, находящихся в директории `/var/www/html` 10
3.11 Пользователи, которым разрешено создание файлов в директории 11
3.12 html-файл и его содержимое 11
3.13 Контекст html-файл 11
3.14 Обращение к файлу через браузер 12
3.15 Выяснение контекста файла 12
3.16 Попытка получить доступ к файлу через веб-сервер 13
3.17 Изменение строки файла 13

Список таблиц

1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. [1]
Проверить работу SELinx на практике совместно с веб-сервером Apache.

2 Задание

1. Подготовить лабораторный стенд и ознакомиться с методическими рекомендациями.
2. С помощью различных примеров ознакомиться с работой SELinux и веб-сервисом Apache.

3 Выполнение лабораторной работы

1. Подготовил лабораторный стенд и ознакомился с методическими рекомендациями.

   Предварительно установил веб-сервис Apache с помощью команды `yum install httpd` (рис - @fig:001).

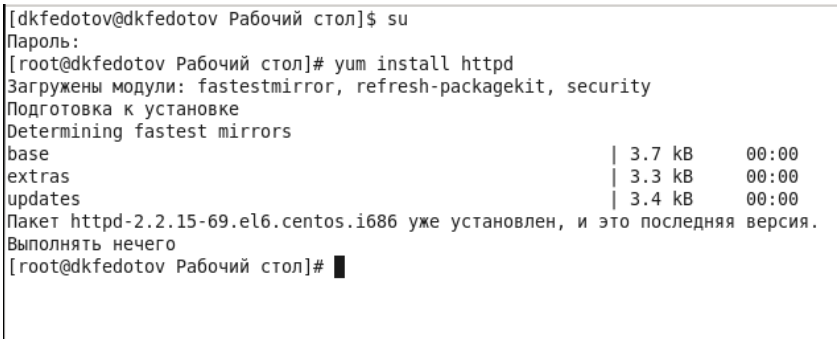

Рис. 3.1: Установка Apache

В конфигурационном файле `/etc/httpd/httpd.conf` задал параметр ServerName: `ServerName test.ru`. Это делается для того, чтобы при запуске веб-сервиса не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе (рис - @fig:002).

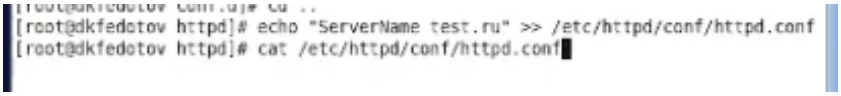

Рис. 3.2: Внемение информации в конфигурационный файл

Также отключил пакетный фильтр (рис - @fig:003).

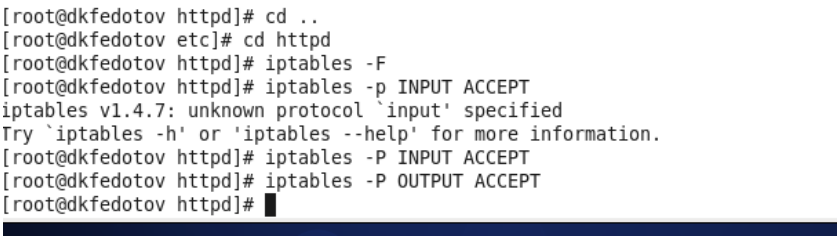

Рис. 3.3: Отключение пакетного фильтра

2. С помощью различных примеров ознакомился с работой SELinux и веб-сервисом Apache.

Вошел в систему с полученными учетными данными и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus` (рис - @fig:004).

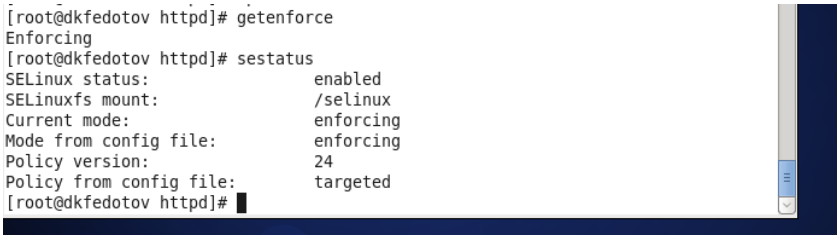

Рис. 3.4: Проверка режима работы SELinux

Обралится с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедился, что последний работает с помощью команды `/etc/rc.d/init.d/httpd status`, предварительно запустив его с помощью команды `/etc/rc.d/init.d/httpd start` (рис - @fig:005).

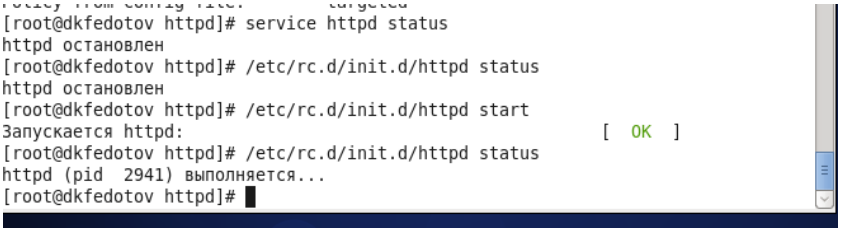

Рис. 3.5: Проверка работы веб-сервера

Нашел веб-сервер Apache в списке процессов и определил его контекст безопасности с помощью команды `ps auxZ | grep httpd` (рис - @fig:006).

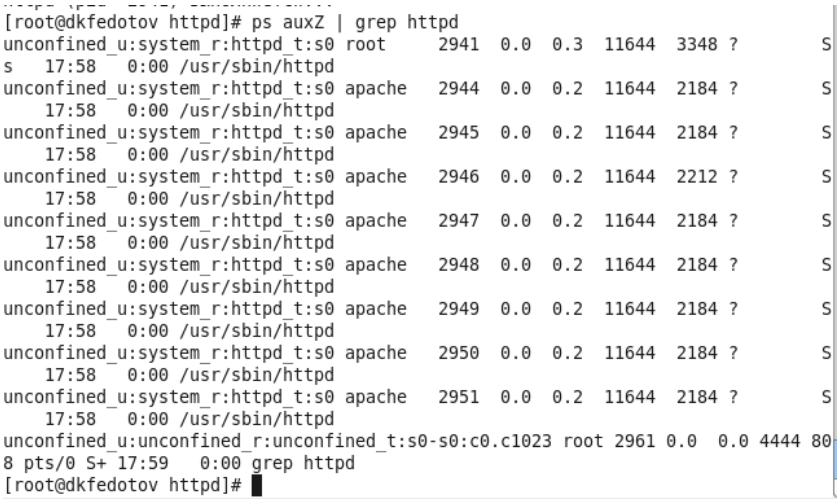

Рис. 3.6: Поиск веб-сервера Apache и определение его контекста безопасности

Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b` (рис - @fig:007).

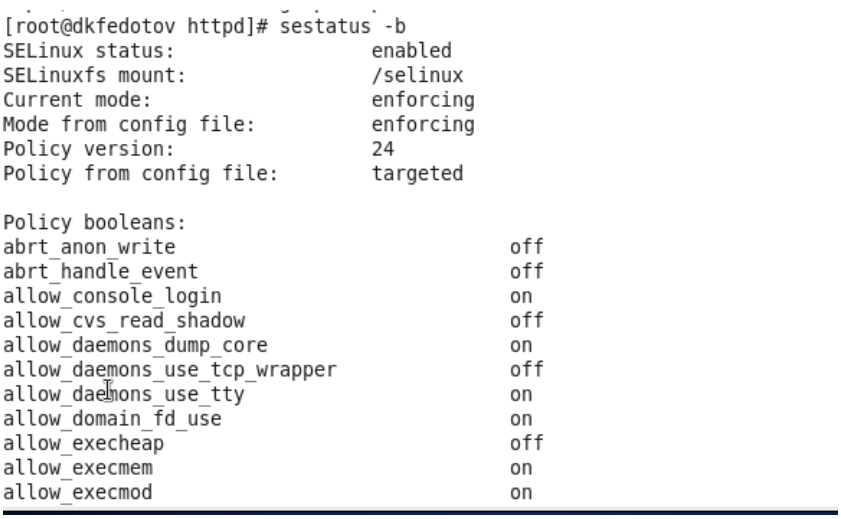

Рис. 3.7: Ттекущее состояние переключателей SELinux для Apache

Посмотрел статистику по политике с помощью команды `seinfo`, а также определил множество пользователей, ролей, типов (рис - @fig:008).

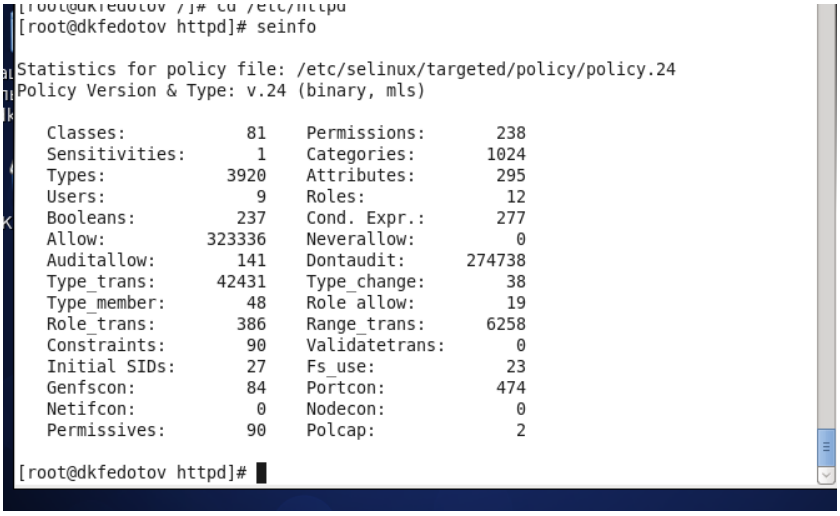

Рис. 3.8: Статистика по политике

Определил тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www` (рис - @fig:009).

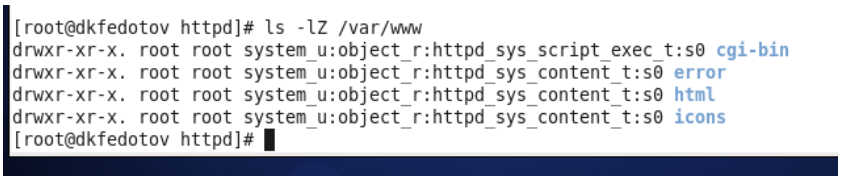

Рис. 3.9: Определение типов файлов и поддиректорий, находящихся в директории `/var/www`

Определил тип файлов, находящихся в директории `/var/www/html` с помощью команды `ls -lZ /var/www/html` (рис - @fig:010).

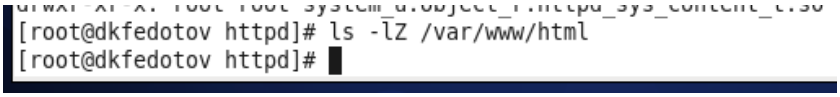

Рис. 3.10: Определение типов файлов и поддиректорий, находящихся в директории `/var/www/html`

Консоль ничего не выводит, поскольку дирректория пуста.

Определил круг пользователей, которым разрешено создание файлов в директории `/var/www/html` (рис - @fig:011).

```
[root@dkfedotov httpd]# ls -l /var/www
итого 16
drwxr-xr-x. 2 root root 4096 Июн 19  2018 cgi-bin
drwxr-xr-x. 3 root root 4096 Окт 16 01:01 error
drwxr-xr-x. 2 root root 4096 Июн 19  2018 html
drwxr-xr-x. 3 root root 4096 Окт 16 01:01 icons
[root@dkfedotov httpd]#
```

Рис. 3.11: Пользователи, которым разрешено создание файлов в директории

Создал от имени суперпользователя html-файл `/var/www/html/test.html` следующего содержания (рис - @fig:012):

*test.html

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

Рис. 3.12: html-файл и его содержимое

Проверил контекст созданного мною файла (рис - @fig:013):

```
[root@dkfedotov httpd]# ls -Z  /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html
/test.html
[root@dkfedotov httpd]#
```

Рис. 3.13: Контекст html-файл

Обратился к файлу через веб-сервис, введя в браузере адрес `http://127.0.0.1/test.html` (рис - @fig:014):

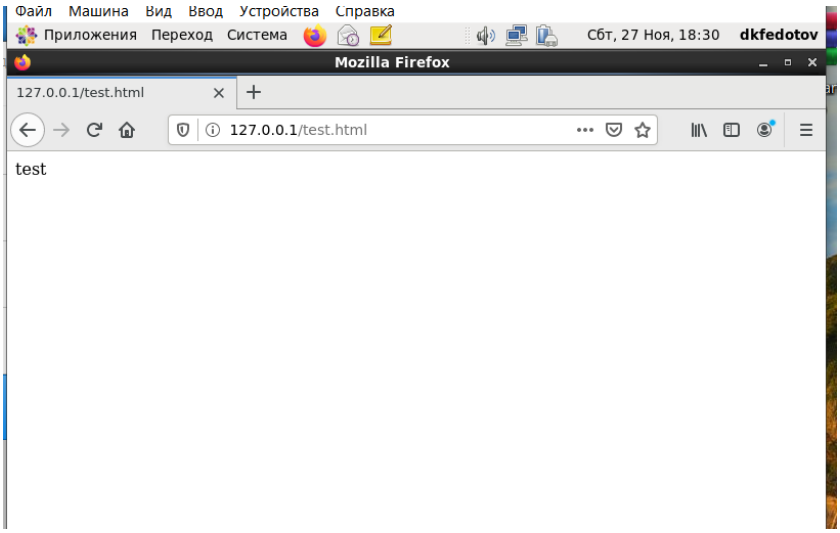

Рис. 3.14: Обращение к файлу через браузер

Проверил контекст файла с помощью команды `ls -Z /var/www/html/test.html` (рис - @fig:015).

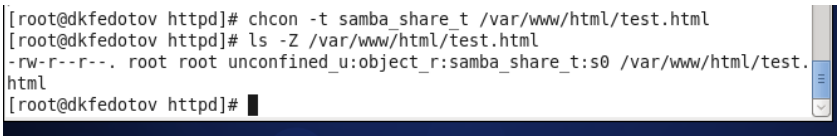

Рис. 3.15: Выяснение контекста файла

Изменил контекст файла `/var/www/html/test.html` с httpd_sys_content_t на samba_share_t.

Попробовал еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получил ошибку (рис - @fig:016).

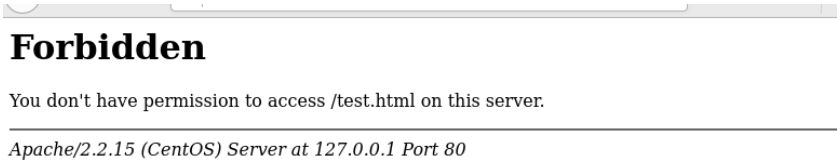

Рис. 3.16: Попытка получить доступ к файлу через веб-сервер

Проанализировал ситуацию. Просмотрел log-файлы веб-сервера Apache, а также посмотрел системный лог-файл с помощью команды `tail /var/log/messages`.

Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле `/etc/httpd/httpd.conf` нашел строчку `Listen 80` и заменил ее на `Listen 81` (рис - @fig:017).

Рис. 3.17: Изменение строки файла

Просмотрел файл /var/log/http/error_log.

Просмотрел файл /var/log/http/access_log.

Просмотрел файл var/log/audit/audit.log.

Выполнил команду semanage port -a -t http_port_t -p tcp 81. После этого проверил список портов командой semanage port -l | grep http_port_t. Убедился, что порт 81 появился в списке.

Вернул контекст httpd_sys_content_t к файлу `/var/www/html/test.html` с помощью команды chcon -t httpd_sys_content_t /var/www/html/test.htmlэ После этого попробовал получить доступ к файлу через веб-сервер, введя в браузере

адрес `http://127.0.0.1:81/test.html`.

Исправил обратно конфигурационный файл apache, вернув `Listen 80`.

Попытался удалить привязку http_port_t к 81 порту.

Удалил файл.

4 Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux.

Проверил работу SELinx на практике совместно с веб-сервером Apache.

5 Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 6. Мандатное разграничение прав в Linux.