Лабораторная работа №6

Основы Информационной Безопасности

Чистов Даниил Максимович

Содержание

Список иллюстраций

1 Цель работы

Целью данной лабораторной работы является развитие навыков администрирования ОС Linux, получение первого практического знакомства с технологией SELinux, проверка работы SELinux на практике совместно с веб-сервером Apache.

2 Выполнение лабораторной работы

Вхожу в систему, убеждаюсь командой sestatus, что SELinux работает в режиме enforcing политики targeted (рис. **??**).

```
[dmchistov@dmchistov conf]$ sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
[dmchistov@dmchistov conf]$ getenforce
Enforcing
[dmchistov@dmchistov conf]$
```

a

Командой service httpd status убеждаюсь, что веб-сервер Apache работает (рис. 2.1).

```
[dmchistov@dmchistov conf]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2025-05-02 18:17:36 MSK; 10min ago
     Docs: man:httpd.service(8)
 Main PID: 42419 (httpd)
   Status: "Running, listening on: port 80"
    Tasks: 213 (limit: 12238)
   Memory: 33.4M
   CGroup: /system.slice/httpd.service
           ├─42419 /usr/sbin/httpd -DFOREGROUND
           ├─42428 /usr/sbin/httpd -DFOREGROUND
           ├─42429 /usr/sbin/httpd -DFOREGROUND
           ├─42430 /usr/sbin/httpd -DFOREGROUND
           └─42431 /usr/sbin/httpd -DFOREGROUND

May 02 18:17:36 dmchistov.localdomain systemd[1]: Starting The Apache HTTP Server...
May 02 18:17:36 dmchistov.localdomain systemd[1]: Started The Apache HTTP Server.
May 02 18:17:36 dmchistov.localdomain httpd[42419]: Server configured, listening on: port 80
[dmchistov@dmchistov conf]$
```

Рис. 2.1: Вывод команды service httpd status

Командой ps auxZ | grep httpd нахожу процессы веб-сервера Apache и определяю

его контекст безопасности - httpd_t (рис. 2.2).

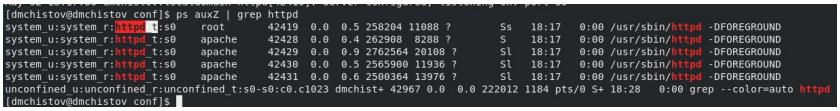

Рис. 2.2: Процессы Apache

Командой sestatus -b | grep httpd смотрю текущее состояние переключателей SELinux для Apaceh, действительно большинство из них в положении “off” (рис. 2.3).

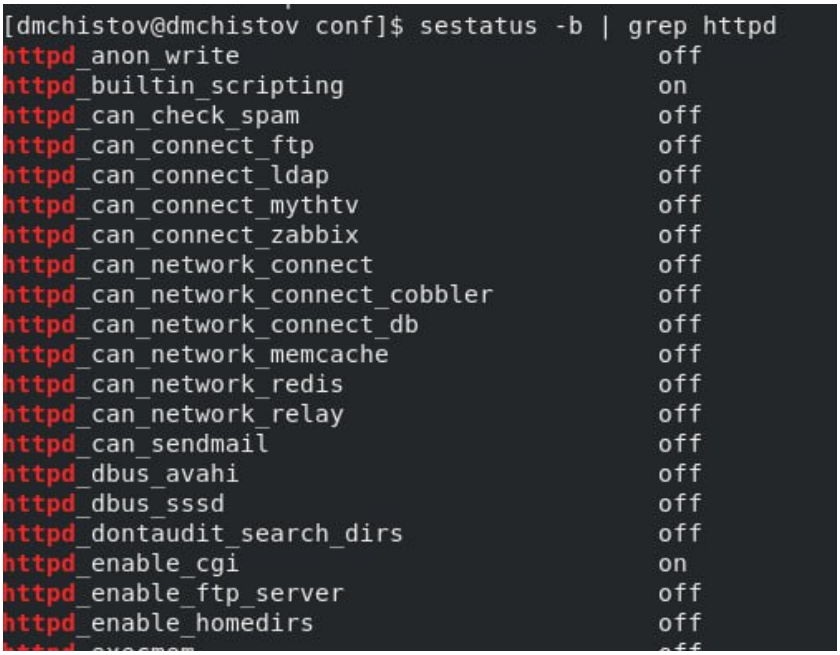

Рис. 2.3: Состояние переключателей SELinux для Apache

Командой seinfo смотрю статистику по политике - вижу, что типов 5015, пользователей - 8, ролей - 15 (рис. 2.4).

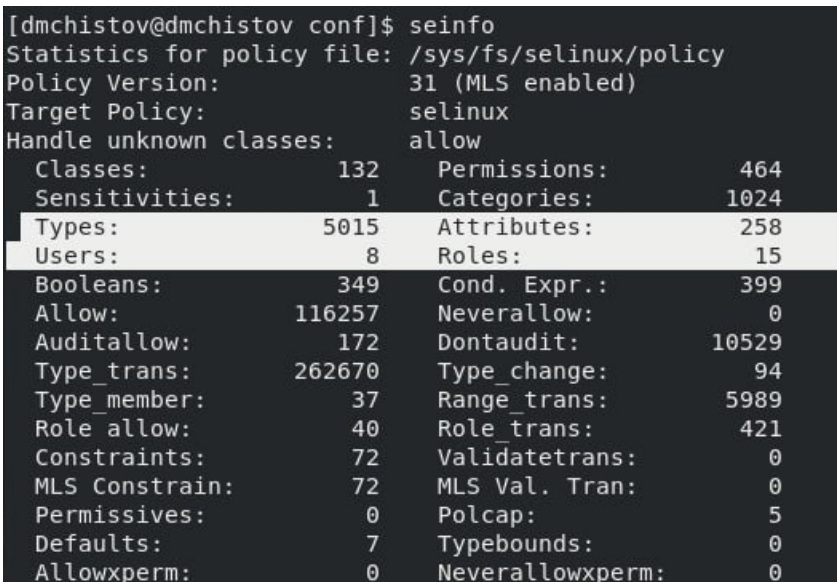

Рис. 2.4: Статистика по политике

Определяю тип файлов и поддиректорий в /var/www, там лежат файлы Apache типа (рис. 2.5).

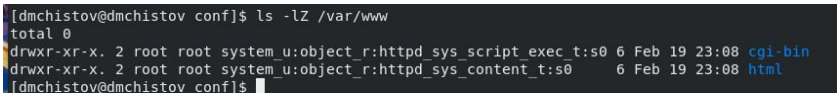

Рис. 2.5: Типы файлов в /var/www

Определяю тип файлов в /var/www/html - нету никаких файлов, также определяю круг пользователей, которым разрешено создание файлов этой директории - только root пользователь на такое способен (рис. 2.6).

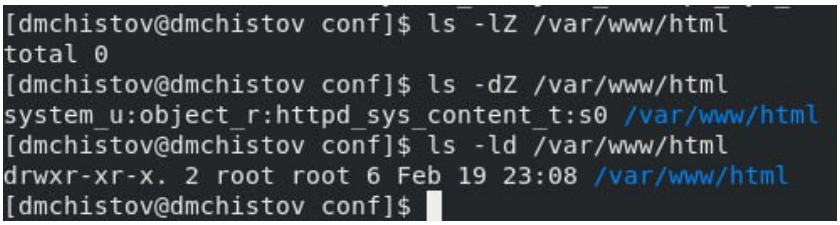

Рис. 2.6: Данные по /var/www/html

От имени суперпользователя создаю html файл test.html - простая веб-страница с текстом - test (рис. 2.7).

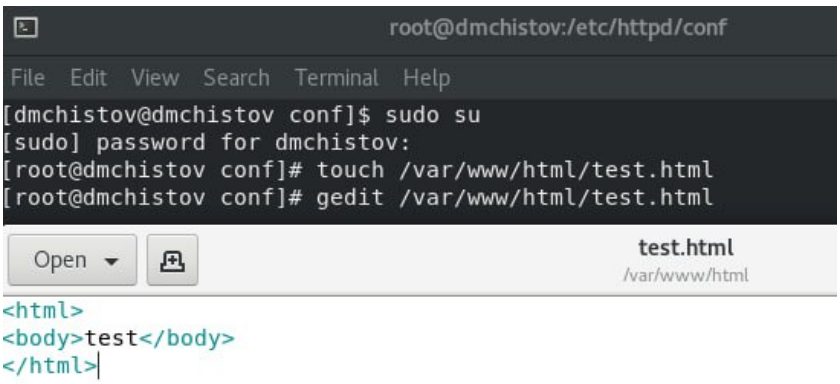

Рис. 2.7: test.html

Проверяю созданный мною файл на контекст - httpd - для Apache (рис. 2.8).

Рис. 2.8: test.html - контекст

Через браузер захожу на эту веб-страничку и вижу соответствующий текст (рис. 2.9).

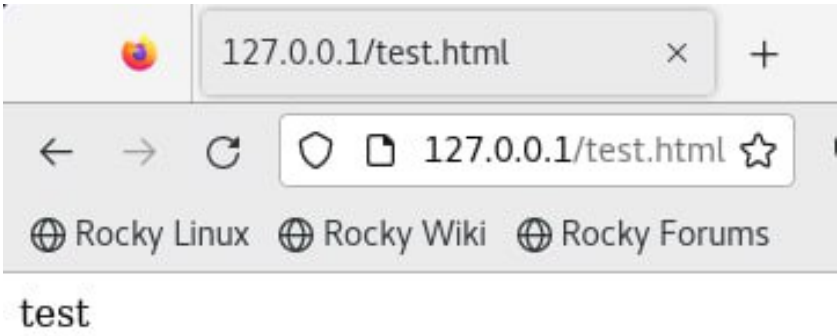

Рис. 2.9: test.html - в браузере

Командой ls -Z /var/www/html/test.html проверяю контекст этого файла - httpd_sys_content_t (такой тип позволяет httpd получить доступ к файлу, поэтому мы можем его открыть через браузер) с unconfined_u (свободный пользователей) (рис. 2.10).

Рис. 2.10: test.html - контекст

Меняю контекст этого файла с httpd_sys_content_t на, например, samra_share_t (рис. 2.11).

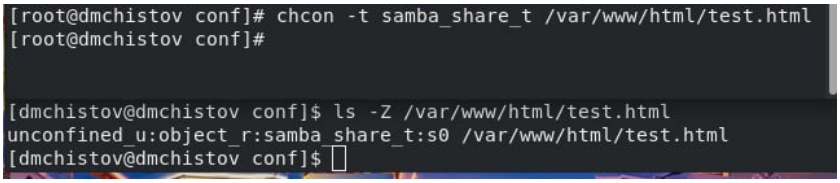

Рис. 2.11: test.html - новый контекст

Пытаюсь заново обратиться к веб-странице через браузер и получаю отказ (рис. 2.12).

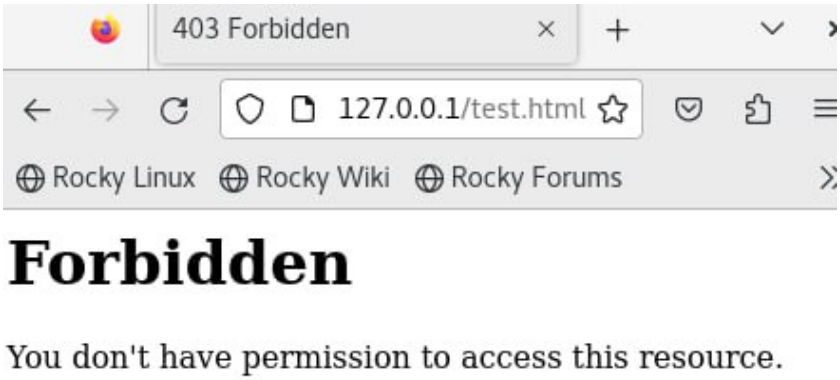

Рис. 2.12: test.html - отказано в доступе

Смотрю лог файлы сервера Apache и пытаюсь разобраться что не так - думаю, дело в том, что мы поменяли тип файла несколькими шагами ранее. Как минимум в логах нас просят поставить какой-то тип данному файлу (рис. 2.13).

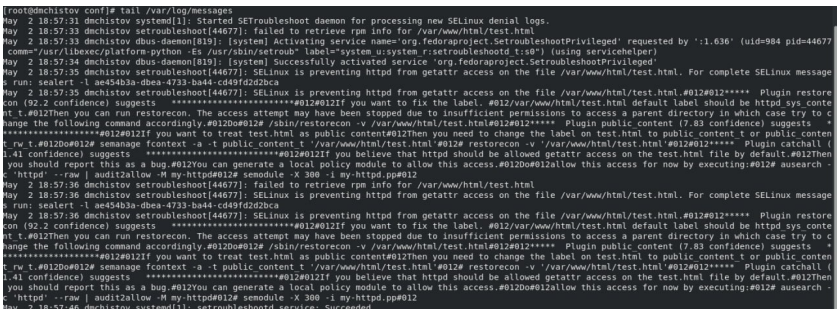

Рис. 2.13: test.html - расследование причины отказа

Запускаю веб-сервер Apache на прослушивании TCP-порта 81, а не 80 - заменяю строку в конфиг файле веб-сервера (рис. 2.14).

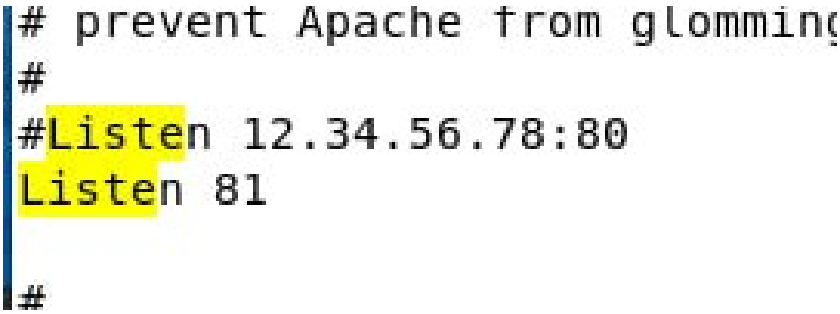

Рис. 2.14: Веб-сервер на прослушивании порта 81

Теперь после перезапуска мне не просто отказано в доступе, а сама страничка уже не грузится (рис. 2.15).

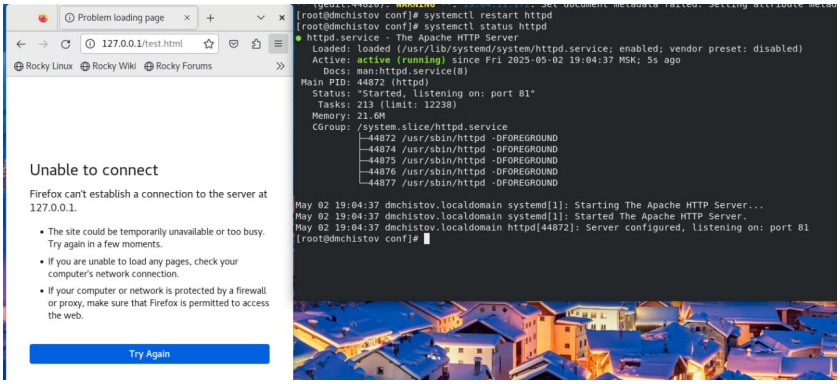

Рис. 2.15: Веб-сервер не загружает страничку

Смотрю лог файлы - сервер прослушивает порт 81 (рис. 2.16).

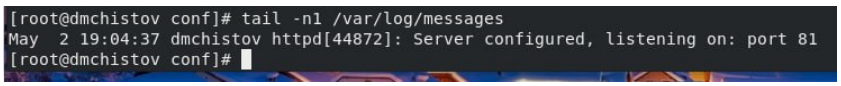

Рис. 2.16: Расследую ситуацию - прослушивание на порте 81

Смотрю другие лог файлы, вижу, что мне говорят об отсутствии прав (рис. 2.17).

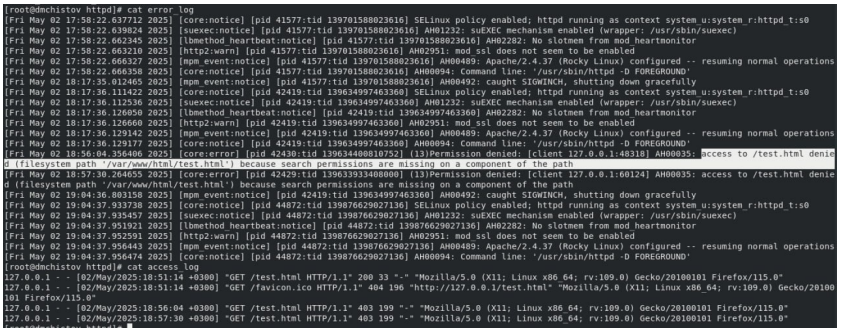

Рис. 2.17: Расследую ситуацию - отсутствие прав

Командой semanage port -a -t http_port_t -p tcp 81 добавляю порт 81, затем смотрю появился ли он - конечно появился (рис. 2.18).

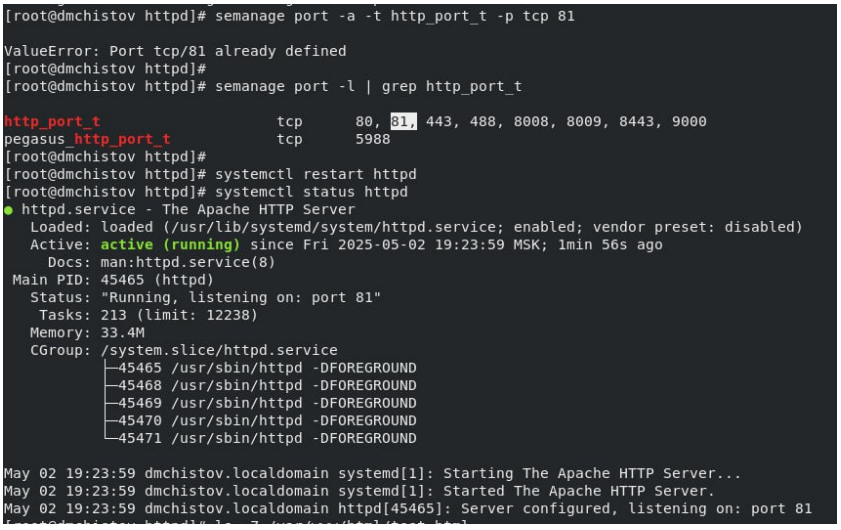

Рис. 2.18: Новый порт - 81

Перезапускаю веб-сервер Apache - всё успешно, нам нужно было объявить ему о новом порте 81, т.к. его не было в списке, а конфиге мы поставили прослушивание этого на тот момент отсутствующего порта. Затем возвращаю нашей

веб-страничке необходимый её тип httpd_sys_content_t и через браузер обращаюсь к той же веб-страничке, но через порт 81 (http://127.0.0.1:81/test.html) - всё работает - текст виден (рис. 2.19).

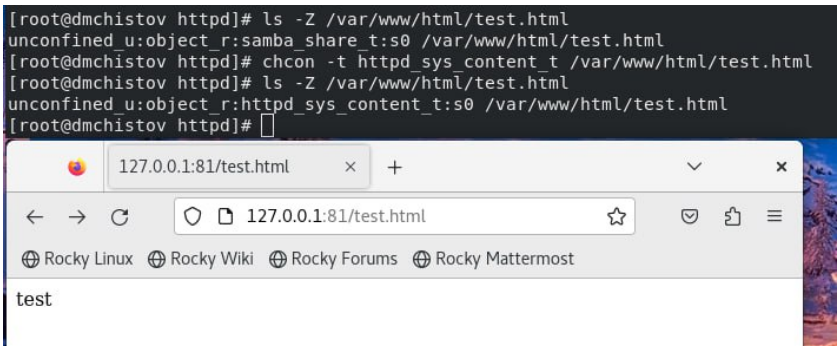

Рис. 2.19: Сайт открывается на порте 81

Завершаю работу - удаляю привязку к порту 81, а также удаляю созданный нами файл test.html (рис. 2.20).

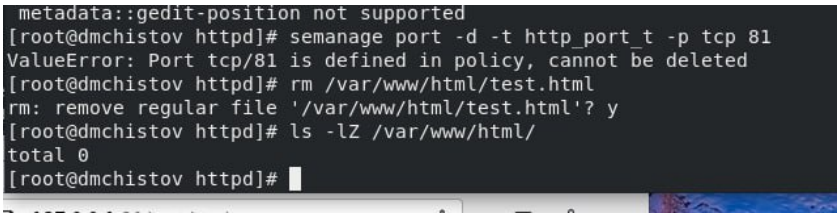

Рис. 2.20: Завершение работы

3 Выводы

В результате выполнения данной лабораторной работы я развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux, проверил работу SELinux на практике совместно с веб-сервером Apache.

4 Список литературы

Лабораторная работа №6