Отчёт по лабораторной работе №6. Мандатное разграничение прав в Linux

Предмет: информационная безопасность

Александр Сергеевич Баклашов

Содержание

List of Figures

1 Цель работы

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

2 Теоретическое введение

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

3 Выполнение лабораторной работы

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus. (рис. 3.1)

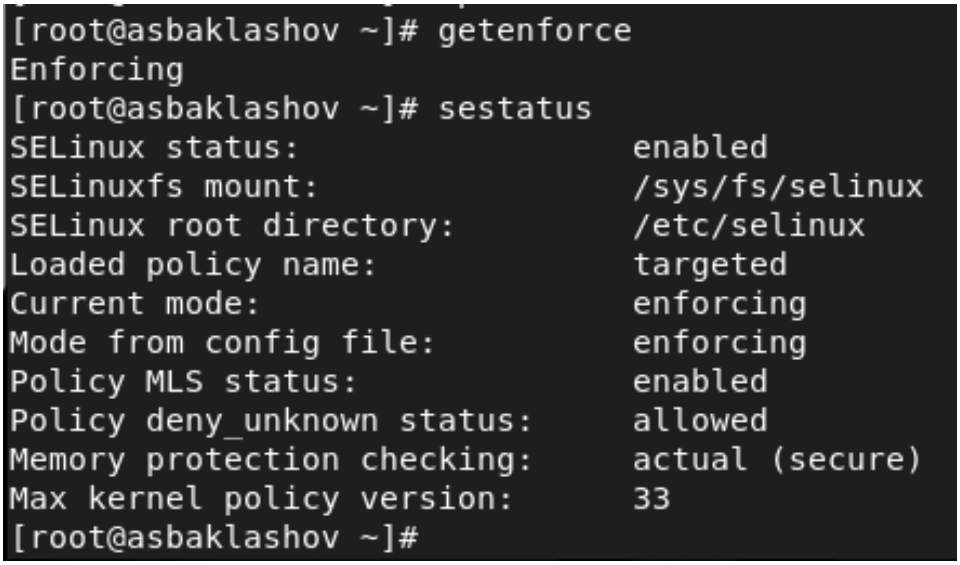

Figure 3.1: getenforce и sestatus

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает (рис. 3.2)

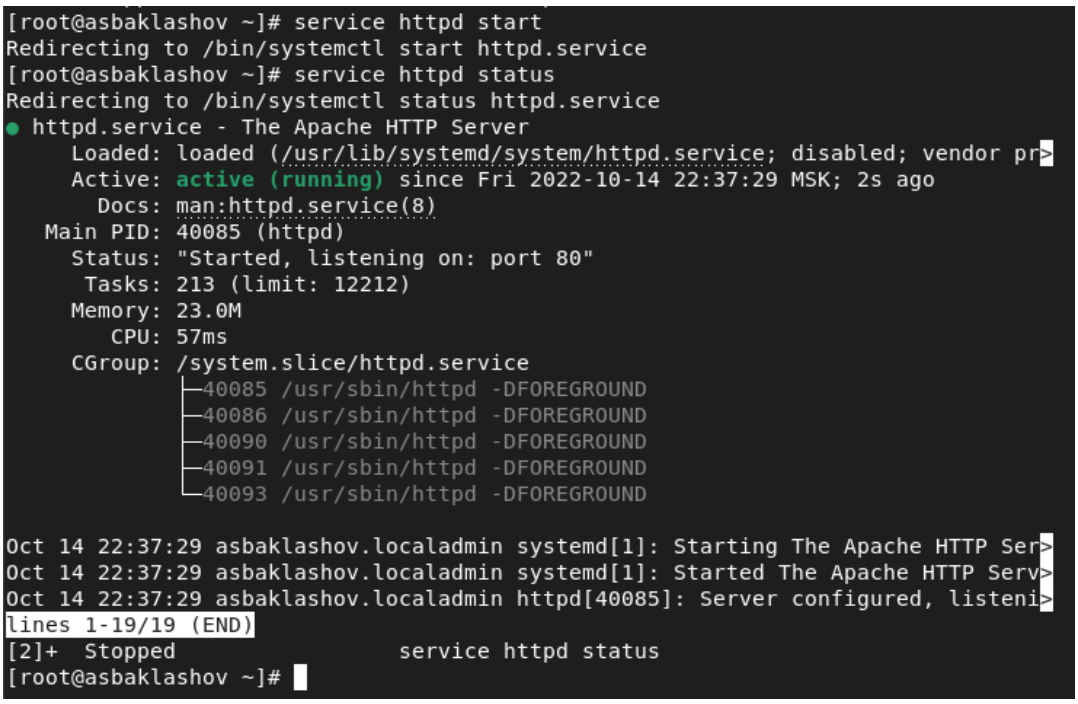

Figure 3.2: Веб-сервер

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. (рис. 3.3)

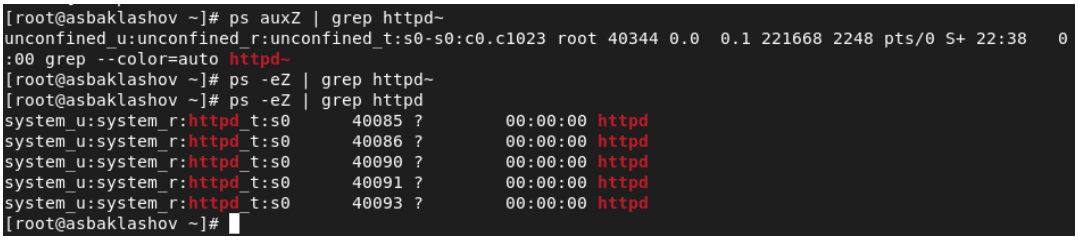

Figure 3.3: Apache

httpd_sys_content_t

4. Посмотрите текущее состояние переключателей SELinux для Apache. (рис. 3.4)

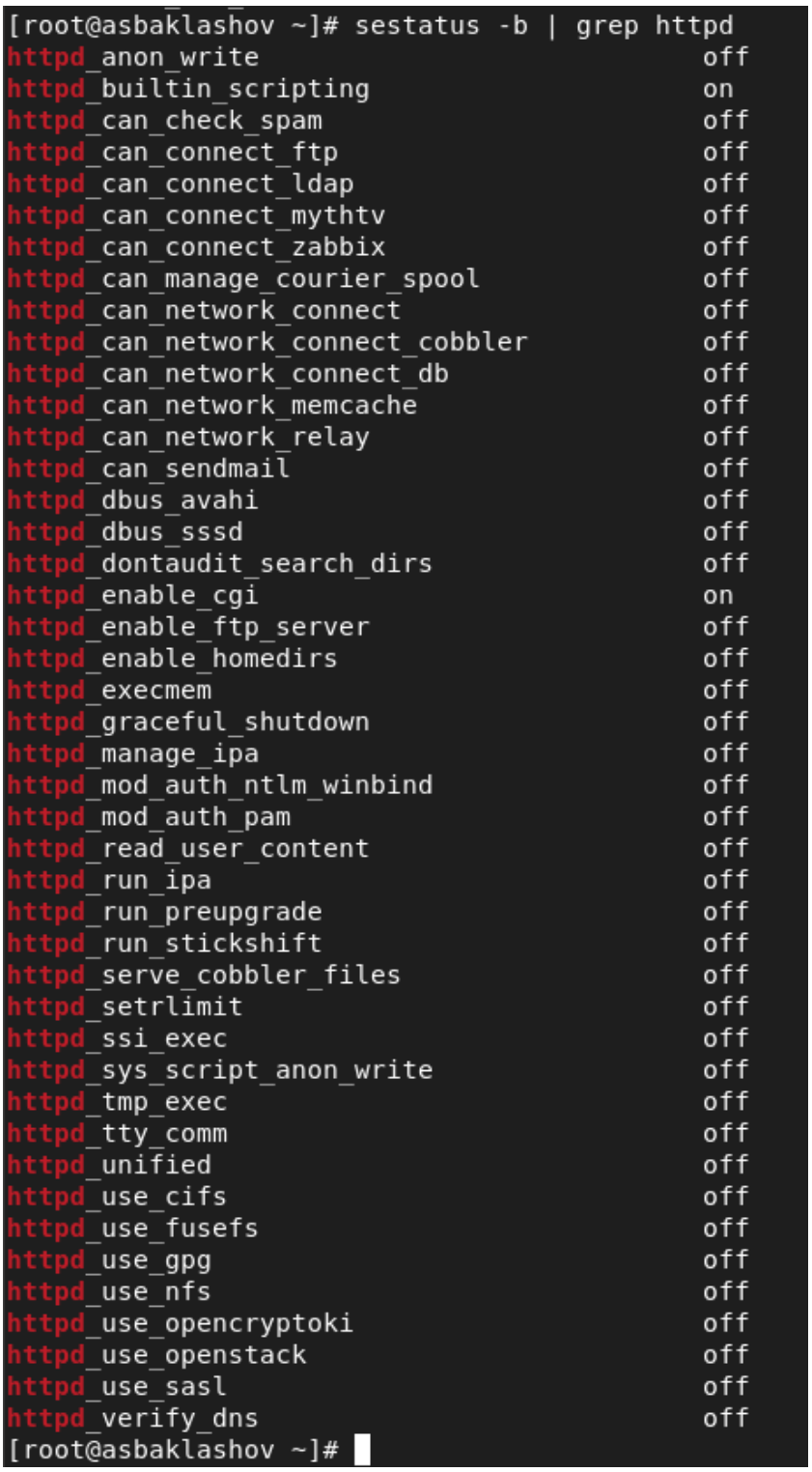

Figure 3.4: Состояние переключателей

5. Посмотрите статистику по политике с помощью команды seinfo, также

определите множество пользователей, ролей, типов. (рис. 3.5)

```
[root@asbaklashov ~]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             33 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:             133    Permissions:         454
  Sensitivities:         1    Categories:         1024
  Types:              4995    Attributes:          254
  Users:                 8    Roles:                14
  Booleans:            347    Cond. Expr.:         382
  Allow:             63727    Neverallow:            0
  Auditallow:          163    Dontaudit:          8391
  Type_trans:       251060    Type_change:          87
  Type_member:          35    Range_trans:        5958
  Role allow:           38    Role_trans:          418
  Constraints:          72    Validatetrans:         0
  MLS Constrain:        72    MLS Val. Tran:         0
  Permissives:           0    Polcap:                5
  Defaults:              7    Typebounds:            0
  Allowxperm:            0    Neverallowxperm:       0
  Auditallowxperm:       0    Dontauditxperm:        0
  Ibendportcon:          0    Ibpkeycon:             0
  Initial SIDs:         27    Fs_use:               33
  Genfscon:            106    Portcon:             651
  Netifcon:              0    Nodecon:               0
[root@asbaklashov ~]#
```

Figure 3.5: seinfo

6. Определите тип файлов и поддиректорий, находящихся в директории /var/www (рис. 3.6)

```
[root@asbaklashov ~]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 May 16 15:10 html
[root@asbaklashov ~]#
```

Figure 3.6: тип

7. Определите тип файлов, находящихся в директории /var/www/html (рис. 3.7)

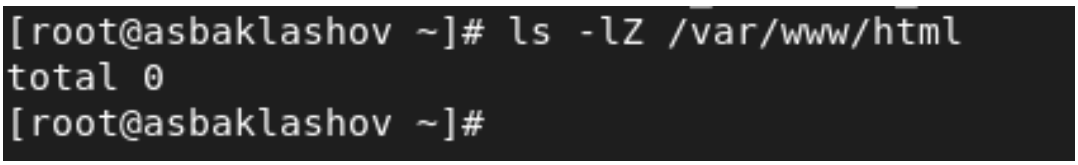

Figure 3.7: тип

8. Определите круг пользователей, которым разрешено создание файлов в директории /var/www/html (рис. 3.8)

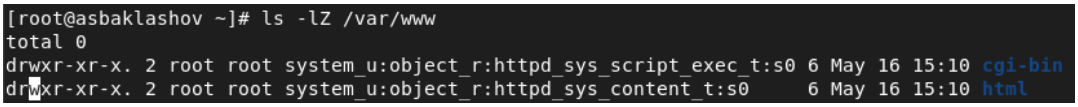

Figure 3.8: круг пользователей

Только владелец

9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

< html >

< body >test< /body >

< /html >

(рис. 3.9)

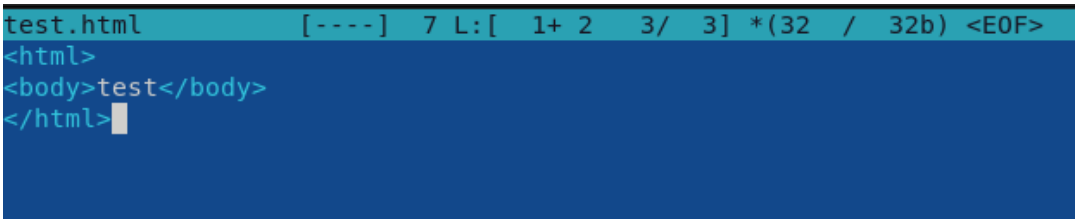

Figure 3.9: файл

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html (рис. 3.10)

```
[root@asbaklashov html]# ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 32 Oct 14 22:54 test.html
[root@asbaklashov html]#
```

Figure 3.10: контекст

httpd_sys_content_t

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён. (рис. 3.11)

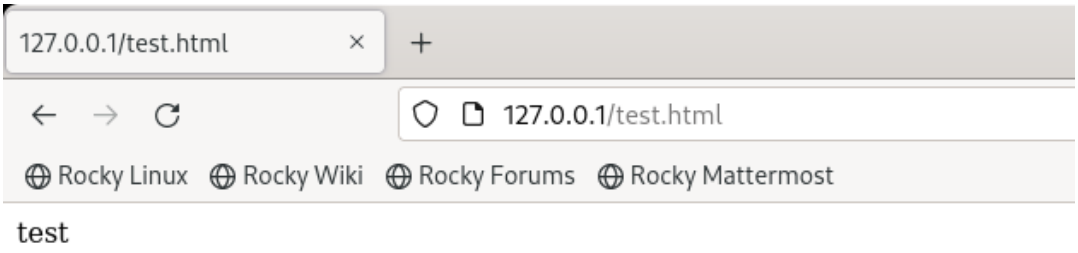

Figure 3.11: http://127.0.0.1/test.html

Файл был успешно отображён

12. Проверить контекст файла /var/www/html/test.html командой ls -Z. ls -Z /var/www/html/test.html (рис. 3.12)

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

Figure 3.12: Проверка

13. Измените контекст файла /var/www/html/test.html с httpd_sys_content_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba_share_t (рис. 3.13)

```
[root@asbaklashov html]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@asbaklashov html]# chcon -t samba_share_t /var/www/html/test.html
[root@asbaklashov html]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@asbaklashov html]#
```

Figure 3.13: Смена контекста

14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Вы должны получить сообщение об ошибке (рис. 3.14)

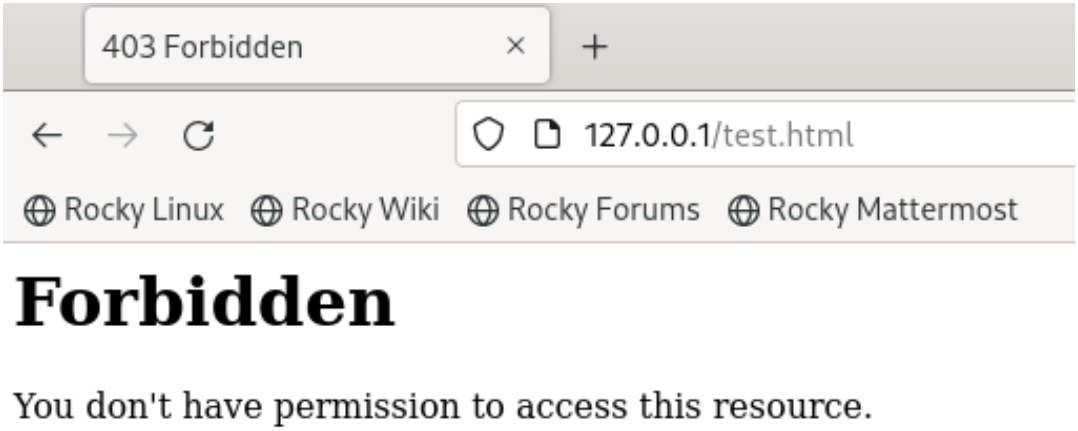

Figure 3.14: Ошибка

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю?

Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: tail /var/log/messages (рис. 3.15)

Figure 3.15: log-файлы

16. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81. (рис. 3.16)

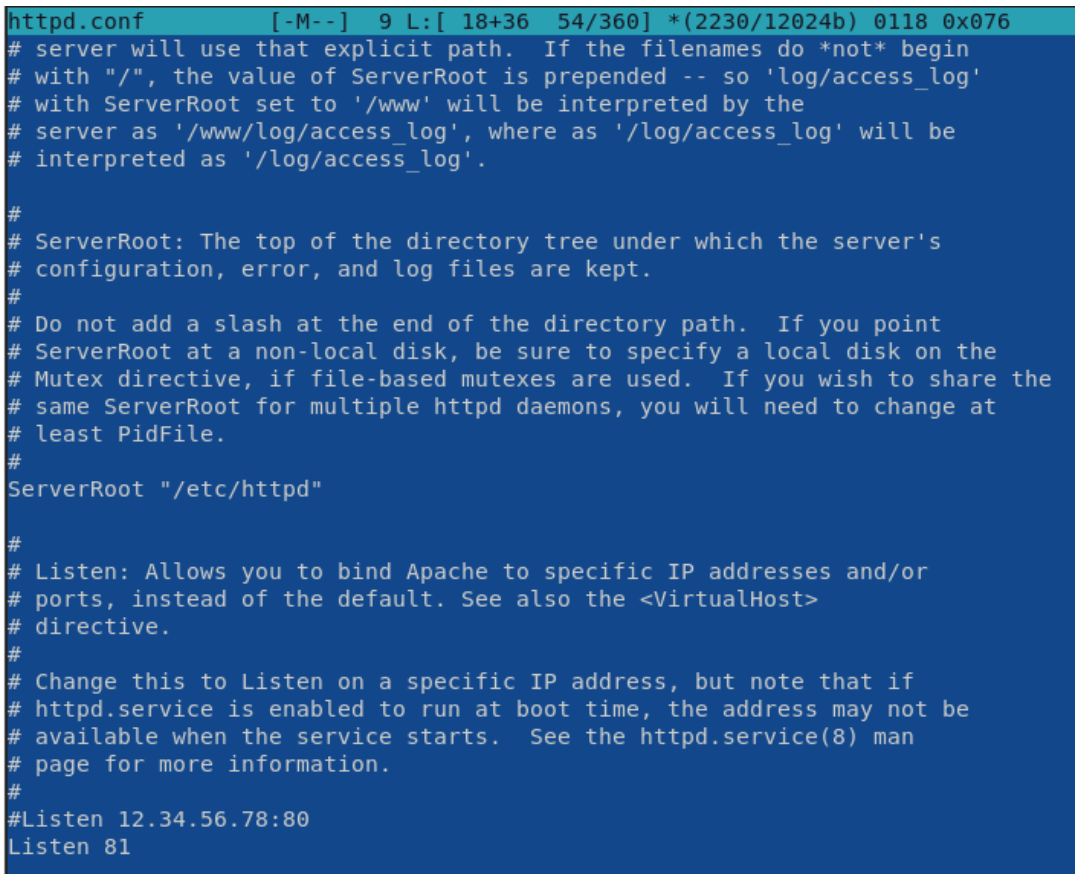

Figure 3.16: Замена

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему?

Сбоя нет.

18. Проанализируйте лог-файлы: tail -nl /var/log/messages Просмотрите файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log и выясните, в каких файлах появились записи. (рис. 3.17, рис. 3.18,рис. 3.19)

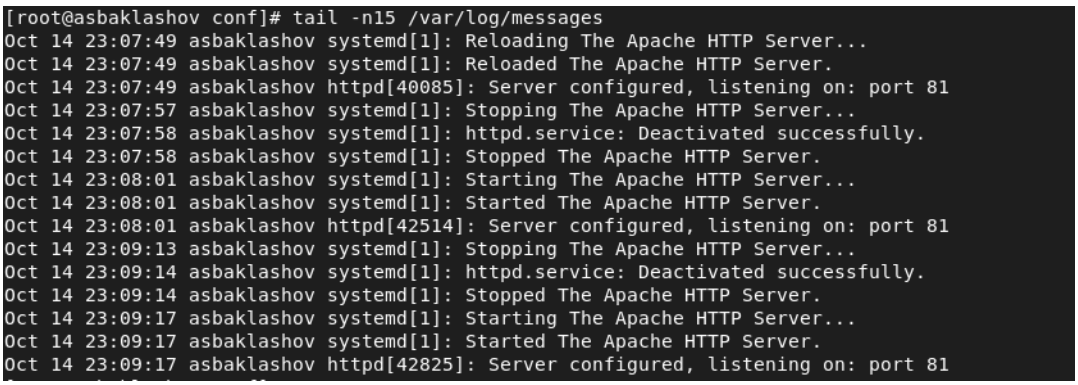

Figure 3.17: /var/log/messages

Figure 3.18: /var/log/http/access_log

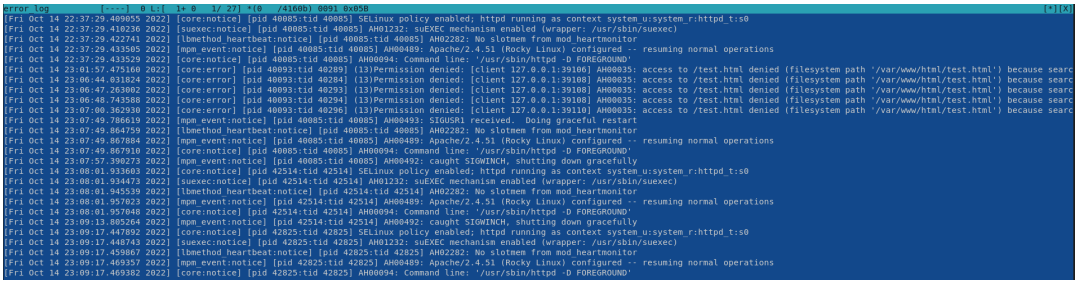

Figure 3.19: /var/log/http/error_log

19. Выполните команду semanage port -a -t http_port_t -p tcp 81

После этого проверьте список портов командой semanage port -l | grep http_port_t Убедитесь, что порт 81 появился в списке. (рис. 3.20)

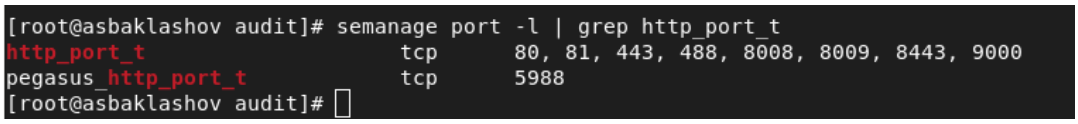

Figure 3.20: 81

Порт 81 был в списке до этого, поэтому сбоя не было.

20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог?

Сервер запускался и до этого. Он бы не запустился, если бы порта 81 изначально не было в списке.

21. Верните контекст httpd_sys_content__t к файлу /var/www/html/ test.html: chcon -t httpd_sys_content_t /var/www/html/test.html После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. Вы должны увидеть содержимое файла — слово «test». (рис. 3.21, рис. 3.22)

Figure 3.21: «test»

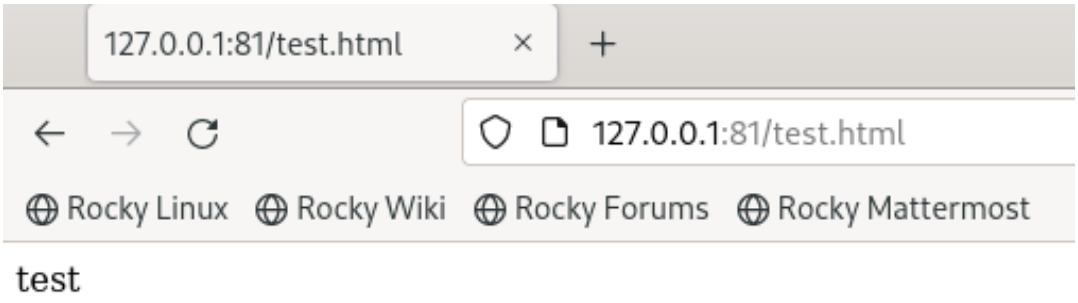

Figure 3.22: «test»

22. Исправьте обратно конфигурационный файл apache, вернув Listen 80. (рис. 3.23)

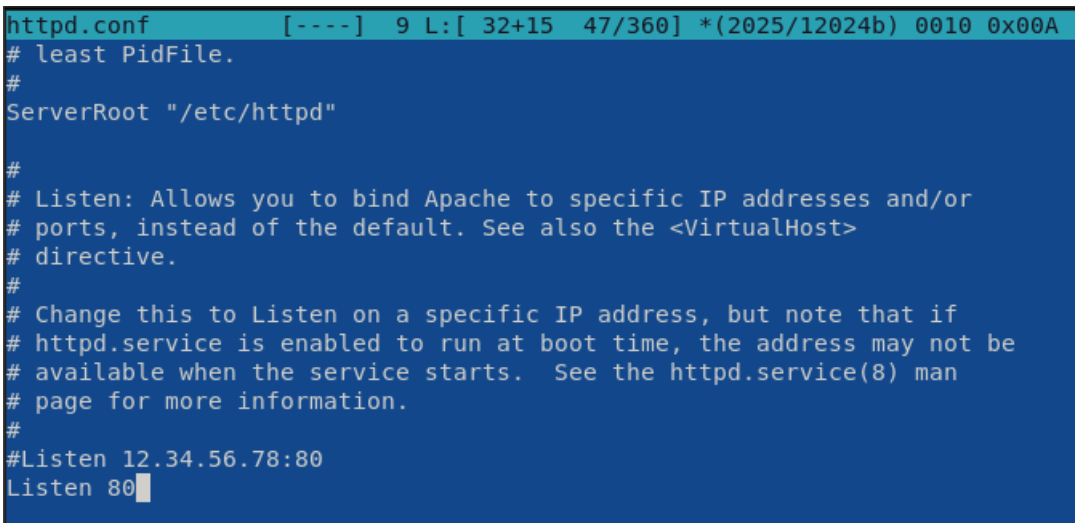

Figure 3.23: Listen 80

23. Удалите привязку http_port_t к 81 порту: semanage port -d -t http_port_t -p tcp 81 (рис. 3.24)

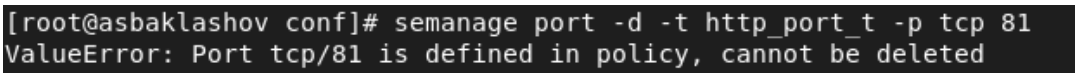

Figure 3.24: 81

Не вышло

24. Удалите файл /var/www/html/test.html (рис. 3.25)

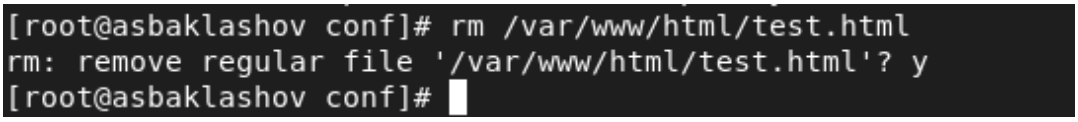

Figure 3.25: Удалите файл

4 Вывод

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

5 Библиография

1. Лабораторная работа № 6. Мандатное разграничение прав в Linux. - 5 с. [Электронный ресурс]. М. URL: Лабораторная работа №6 (Дата обращения: 15.10.2022).

2. Rocky Linux Documentation. [Электронный ресурс]. М. URL: Rocky Linux Documentation (Дата обращения: 15.10.2022).