

Лабораторная работа №6

Мандатное разграничение прав в Linux

Щербак Маргарита Романовна, НПИбд-02-21

2024

Содержание

Цель работы	4
Теоретическое введение	5
Выполнение лабораторной работы	6
Вывод	24
Библиография	25

Список иллюстраций

1	getenforce и sestatus	6
2	Веб-сервер httpd	7
3	Веб-сервер Apache	8
4	Состояние переключателей	9
5	Статистика по политике с помощью команды seinfo	10
6	Просмотр типов файлов и поддиректорий	11
7	Содержимое файла	12
8	Контекст и отображение файла	13
9	Проверка контекста и его изменение	14
10	Ошибка	15
11	log-файлы	16
12	log-файлы	17
13	Замена порта в файле	18
14	/var/log/messages	19
15	/var/log/http/access_log	20
16	/var/log/http/error_log	21
17	Semanage и запуск веб-сервера	22
18	Удаление файла	23

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].

Теоретическое введение

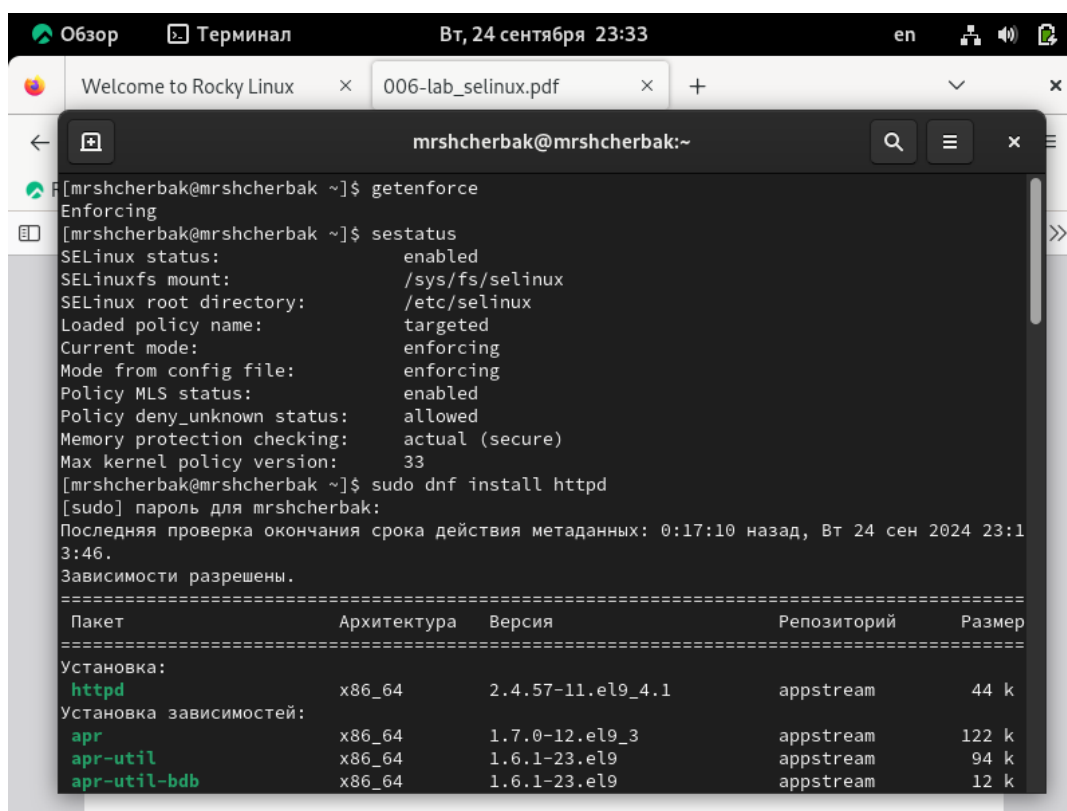
Информационная безопасность представляет собой защиту данных и поддерживающей инфраструктуры от случайных или преднамеренных воздействий природного или искусственного характера, которые могут нанести ущерб владельцам или пользователям этой информации и инфраструктуры [1].

Мандатное разграничение прав (Mandatory Access Control, MAC) — это метод управления доступом, где права пользователей и процессов определяются на системном уровне и не могут быть изменены без административного вмешательства. В отличие от дискреционного контроля доступа (DAC), где пользователи могут самостоятельно устанавливать права на свои файлы, MAC жестко контролирует доступ к ресурсам на основании политик безопасности [2].

SELinux (Security-Enhanced Linux) — это система MAC в Linux, которая реализует разграничение прав через политики безопасности [3].

Выполнение лабораторной работы

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



```
[mrshcherbak@mrshcherbak ~]$ getenforce
Enforcing
[mrshcherbak@mrshcherbak ~]$ 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
[mrshcherbak@mrshcherbak ~]$ sudo dnf install httpd
[sudo] пароль для mrshcherbak:
Последняя проверка окончания срока действия метаданных: 0:17:10 назад, Вт 24 сен 2024 23:13:46.
Зависимости разрешены.
=====
Пакет                Архитектура  Версия                Репозиторий          Размер
=====
Установка:
  httpd              x86_64       2.4.57-11.el9_4.1     appstream             44 k
Установка зависимостей:
  apr                x86_64       1.7.0-12.el9_3        appstream             122 k
  apr-util            x86_64       1.6.1-23.el9          appstream             94 k
  apr-util-bdb        x86_64       1.6.1-23.el9          appstream             12 k
```

Рис. 1: `getenforce` и `sestatus`

2. Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает (рис.2).

The screenshot shows a web browser window with two tabs: 'Welcome to Rocky Linux' and '006-lab_selinux.pdf'. The active tab displays a terminal window titled 'mrshcherbak@mrshcherbak:~ — /bin/systemctl status httpd.service'. The terminal output shows the following commands and results:

```
Выполнено!  
[mrshcherbak@mrshcherbak ~]$ service httpd start  
Redirecting to /bin/systemctl start httpd.service  
[mrshcherbak@mrshcherbak ~]$ service httpd status  
Redirecting to /bin/systemctl status httpd.service  
● httpd.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)  
   Active: active (running) since Tue 2024-09-24 23:31:44 MSK; 2min 23s ago  
     Docs: man:httpd.service(8)  
  Main PID: 33537 (httpd)  
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/se  
    Tasks: 177 (limit: 24675)  
   Memory: 30.0M  
      CPU: 232ms  
   CGroup: /system.slice/httpd.service  
           └─33537 /usr/sbin/httpd -DFOREGROUND  
             └─33631 /usr/sbin/httpd -DFOREGROUND  
               └─33636 /usr/sbin/httpd -DFOREGROUND  
                 └─33637 /usr/sbin/httpd -DFOREGROUND  
                   └─33638 /usr/sbin/httpd -DFOREGROUND  
  
сен 24 23:31:44 mrshcherbak systemd[1]: Starting The Apache HTTP Server...  
сен 24 23:31:44 mrshcherbak httpd[33537]: AH00558: httpd: Could not reliably determine th  
сен 24 23:31:44 mrshcherbak systemd[1]: Started The Apache HTTP Server.  
сен 24 23:31:44 mrshcherbak httpd[33537]: Server configured, listening on: port 80  
lines 1-20/20 (END)
```

Рис. 2: Веб-сервер httpd

3. Нашла веб-сервер Apache в списке процессов. Его контекст безопасности `httpd_sys_content_t` (рис.3).

```
Обзор Терминал Вт, 24 сентября 23:37 en
mrshcherbak@mrshcherbak:~

Memory: 30.0M
CPU: 232ms
CGroup: /system.slice/httpd.service
├─33537 /usr/sbin/httpd -DFOREGROUND
├─33631 /usr/sbin/httpd -DFOREGROUND
├─33636 /usr/sbin/httpd -DFOREGROUND
├─33637 /usr/sbin/httpd -DFOREGROUND
└─33638 /usr/sbin/httpd -DFOREGROUND

сен 24 23:31:44 mrshcherbak systemd[1]: Starting The Apache HTTP Server...
сен 24 23:31:44 mrshcherbak httpd[33537]: AH00558: httpd: Could not reliably determine the
сен 24 23:31:44 mrshcherbak systemd[1]: Started The Apache HTTP Server.
сен 24 23:31:44 mrshcherbak httpd[33537]: Server configured, listening on: port 80
lines 1-20/20 (END)
[mrshcherbak@mrshcherbak ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 33537 0.0 0.2 20364 11488 ? Ss 23:31 0:00 /usr/sbin/htt
pd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 33631 0.0 0.1 22096 7248 ? S 23:31 0:00 /usr/sbin/htt
pd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 33636 0.0 0.5 1112656 21596 ? Sl 23:31 0:00 /usr/sbin/htt
pd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 33637 0.0 0.2 981520 11160 ? Sl 23:31 0:00 /usr/sbin/htt
pd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 33638 0.0 0.2 981520 11160 ? Sl 23:31 0:00 /usr/sbin/htt
pd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0.c1023 mrshche+ 41858 0.0 0.0 221820 2432 pts/0 S+ 23:35 0:00
grep --color=auto httpd
[mrshcherbak@mrshcherbak ~]$ ps auxZ | grep httpd~
unconfined_u:unconfined_r:unconfined_t:s0-c0.c1023 mrshche+ 41864 0.0 0.0 221688 2304 pts/0 S+ 23:35 0:00
grep --color=auto httpd-
[mrshcherbak@mrshcherbak ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 33537 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 33631 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 33636 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 33637 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 33638 ? 00:00:00 httpd
[mrshcherbak@mrshcherbak ~]$
```

Рис. 3: Веб-сервер Apache

4. Посмотрела текущее состояние переключателей SELinux для Apache (рис.4).

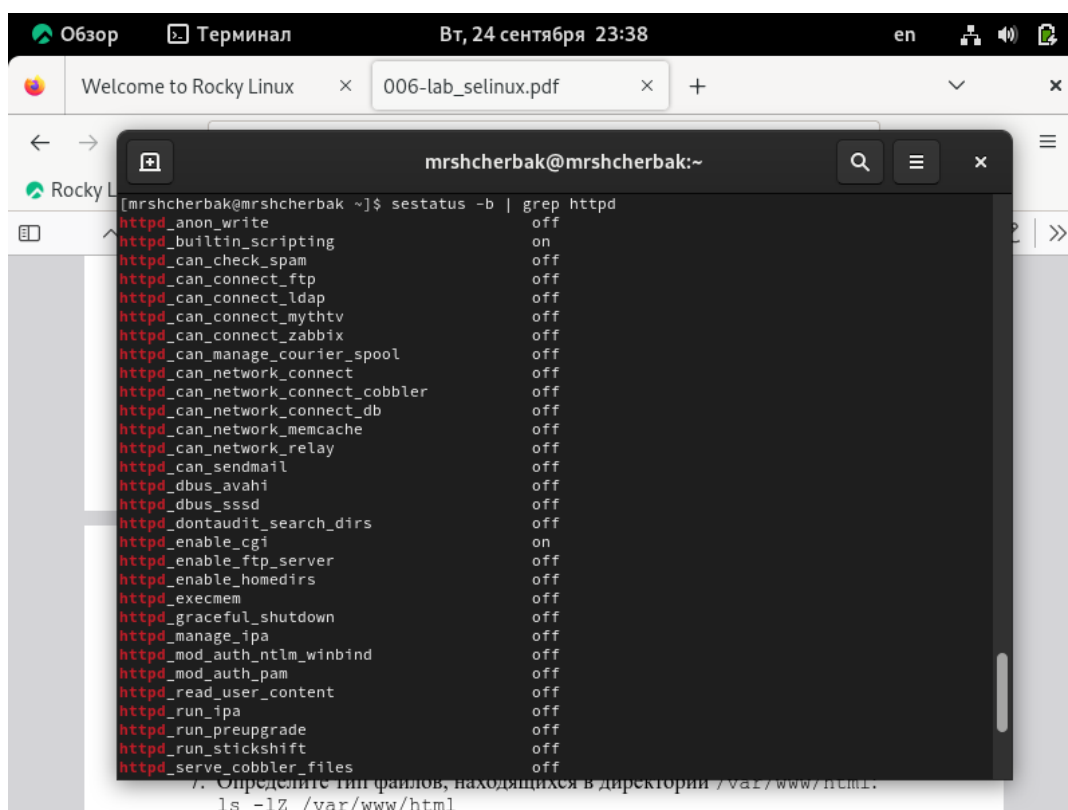


Рис. 4: Состояние переключателей

5. Посмотрела статистику по политике с помощью команды `seinfo`, также определила множество пользователей, ролей, типов (рис.5).

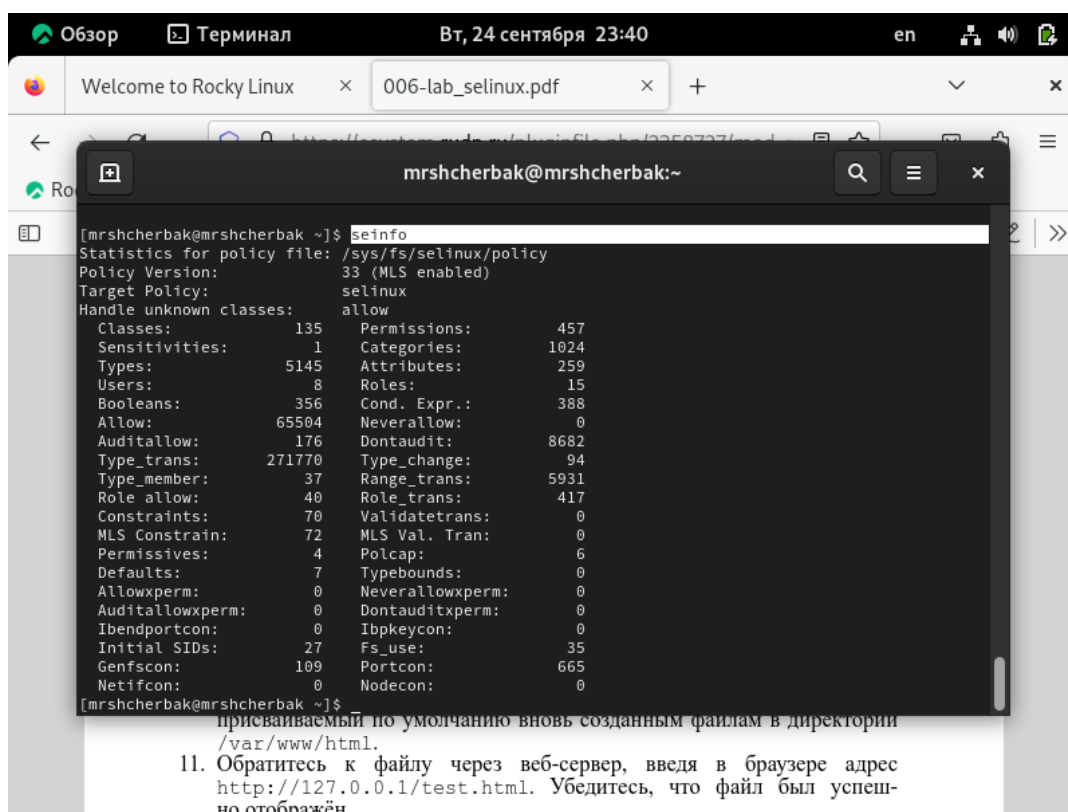


Рис. 5: Статистика по политике с помощью команды seinfo

6. Определила тип файлов и поддиректорий, находящихся в директории /var/www. Определила тип файлов, находящихся в директории /var/www/html. Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html - только владелец (рис.6).

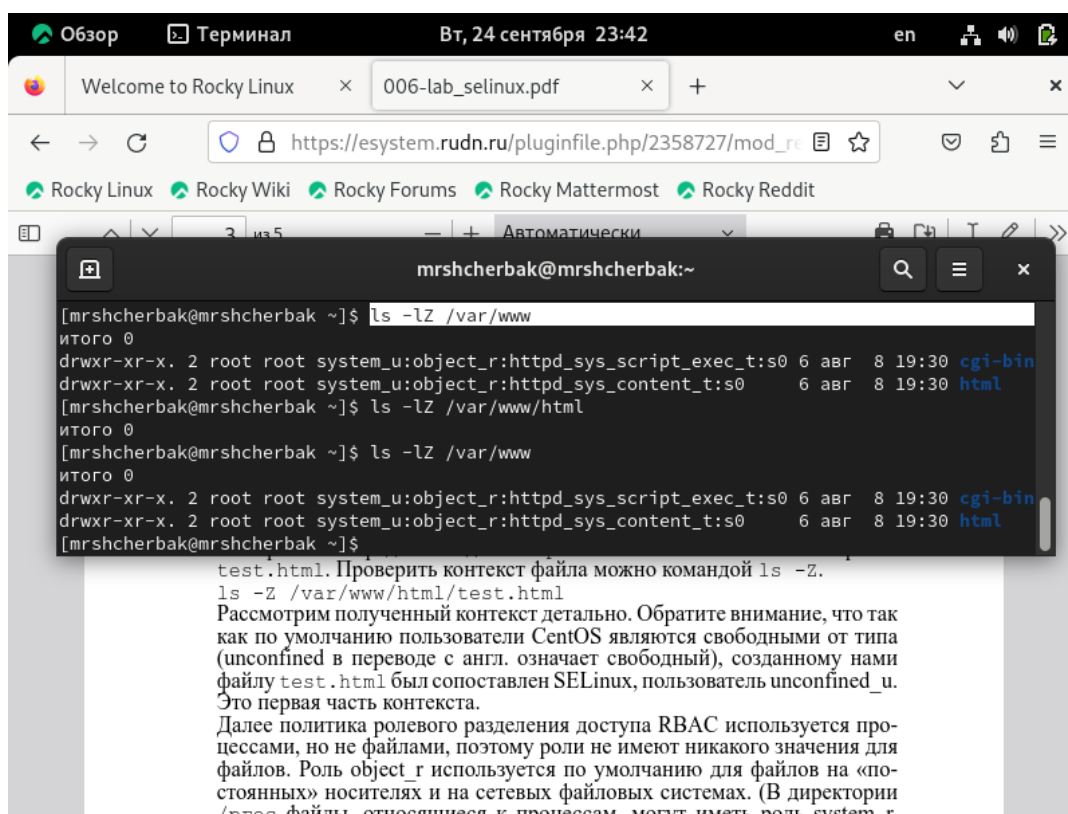


Рис. 6: Просмотр типов файлов и поддиректорий

7. Создала от имени суперпользователя html-файл `/var/www/html/test.html` следующего содержания. А также проверила контекст созданного файла - `httpd_sys_content_t` (рис.7).

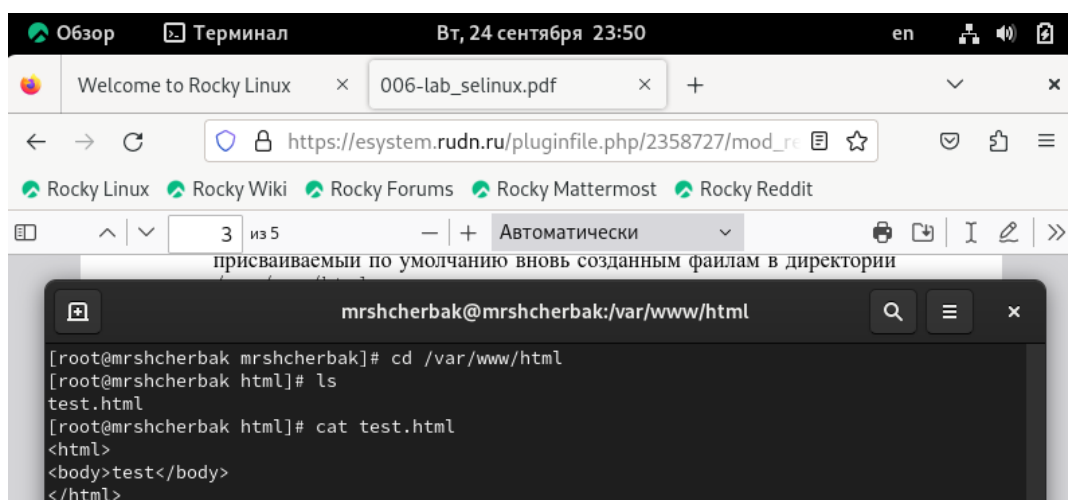
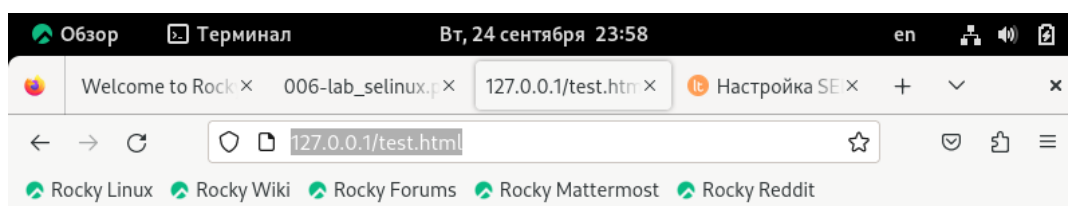


Рис. 7: Содержимое файла

8. Проверила контекст созданного файла. Обратилась к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедилась, что файл был успешно отображён (рис.8). Файл был успешно отображён.



test

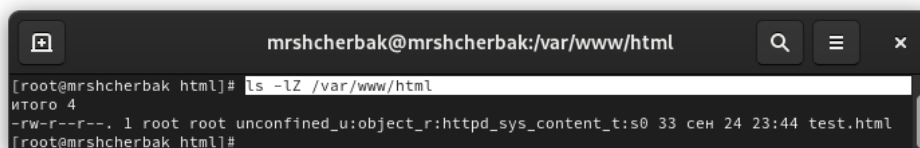


Рис. 8: Контекст и отображение файла

9. Проверила контекст файла `/var/www/html/test.html` командой `ls -Z`. Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t` (рис.9).

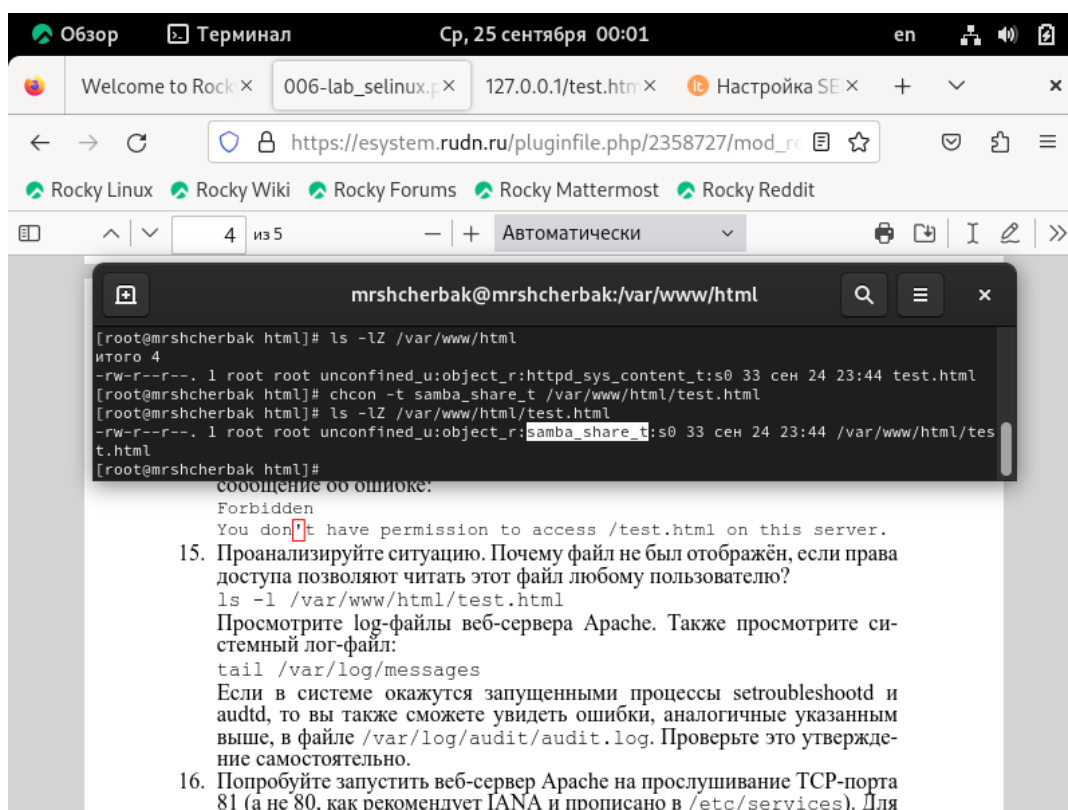
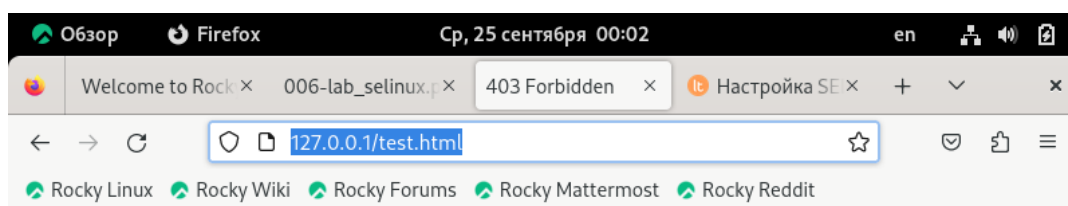


Рис. 9: Проверка контекста и его изменение

10. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получила сообщение об ошибке (рис.10).

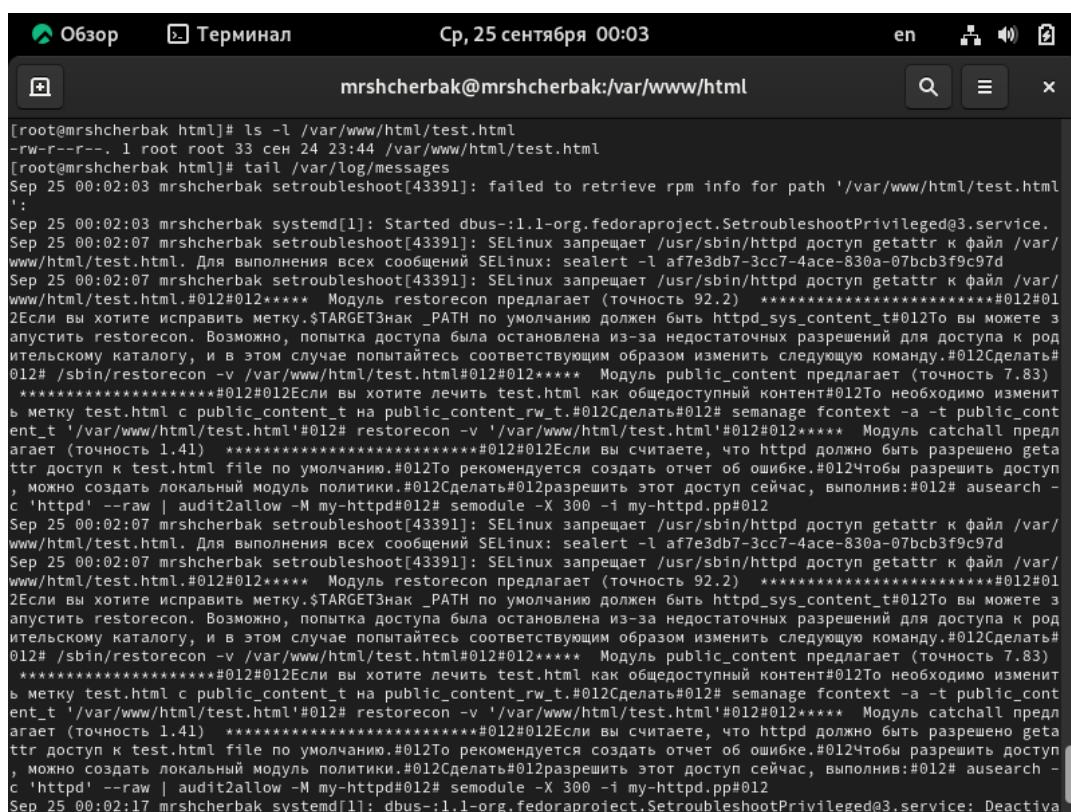


Forbidden

You don't have permission to access this resource.

Рис. 10: Ошибка

11. Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл: `tail /var/log/messages` (рис.11 - рис.12).



```
[root@mrshcherbak html]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 сен 24 23:44 /var/www/html/test.html
[root@mrshcherbak html]# tail /var/log/messages
Sep 25 00:02:03 mrshcherbak setroubleshoot[43391]: failed to retrieve rpm info for path '/var/www/html/test.html'
Sep 25 00:02:03 mrshcherbak systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@3.service.
Sep 25 00:02:07 mrshcherbak setroubleshoot[43391]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/
www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l af7e3db7-3cc7-4ace-830a-07bcb3f9c97d
Sep 25 00:02:07 mrshcherbak setroubleshoot[43391]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/
www/html/test.html.#012#012***** Модуль restorecon предлагает (точность 92.2) *****#012#01
2Если вы хотите исправить метку.$TARGETЗнак _PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете з
апустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для доступа к род
ительскому каталогу, и в этом случае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#
012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Модуль public_content предлагает (точность 7.83)
*****#012#012Если вы хотите лечить test.html как общедоступный контент#012То необходимо изменит
ь метку test.html с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t public_cont
ent_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Модуль catchall предл
агает (точность 1.41) *****#012#012Если вы считаете, что httpd должно быть разрешено geta
ttr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ
, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -
с 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Sep 25 00:02:07 mrshcherbak setroubleshoot[43391]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/
www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l af7e3db7-3cc7-4ace-830a-07bcb3f9c97d
Sep 25 00:02:07 mrshcherbak setroubleshoot[43391]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/
www/html/test.html.#012#012***** Модуль restorecon предлагает (точность 92.2) *****#012#01
2Если вы хотите исправить метку.$TARGETЗнак _PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете з
апустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для доступа к род
ительскому каталогу, и в этом случае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#
012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Модуль public_content предлагает (точность 7.83)
*****#012#012Если вы хотите лечить test.html как общедоступный контент#012То необходимо изменит
ь метку test.html с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t public_cont
ent_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Модуль catchall предл
агает (точность 1.41) *****#012#012Если вы считаете, что httpd должно быть разрешено geta
ttr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ
, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -
с 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Sep 25 00:02:17 mrshcherbak systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@3.service: Deactiva
```

Рис. 11: log-файлы

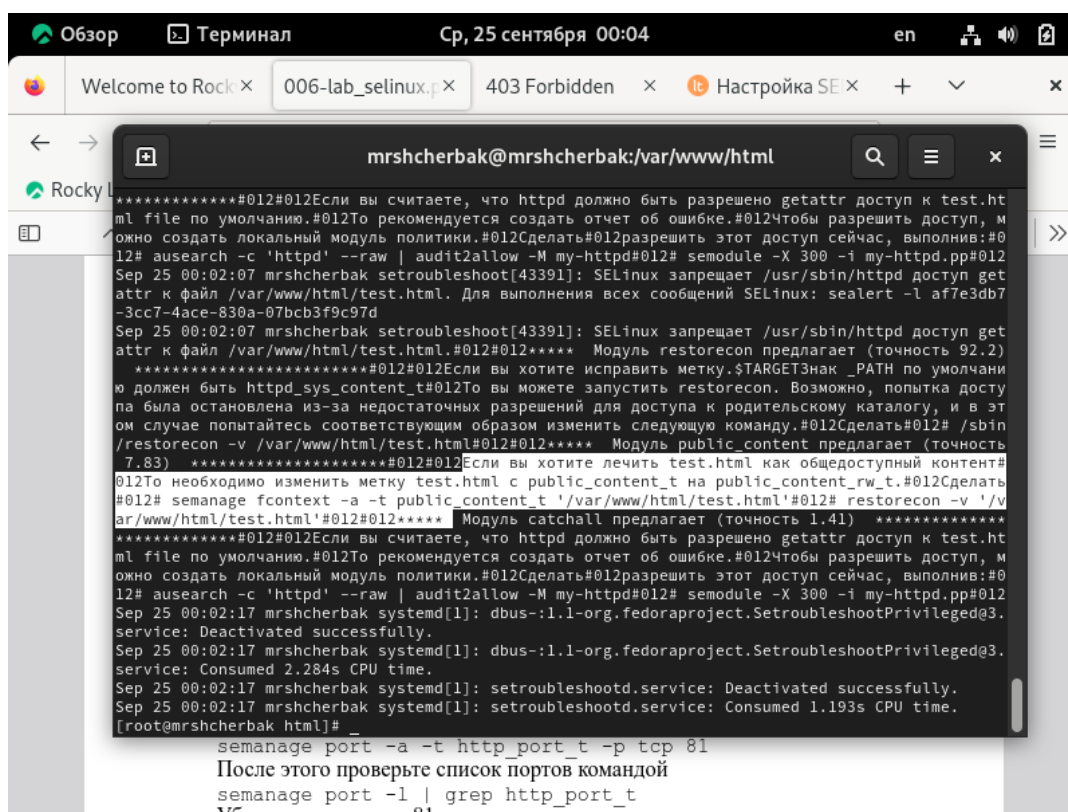
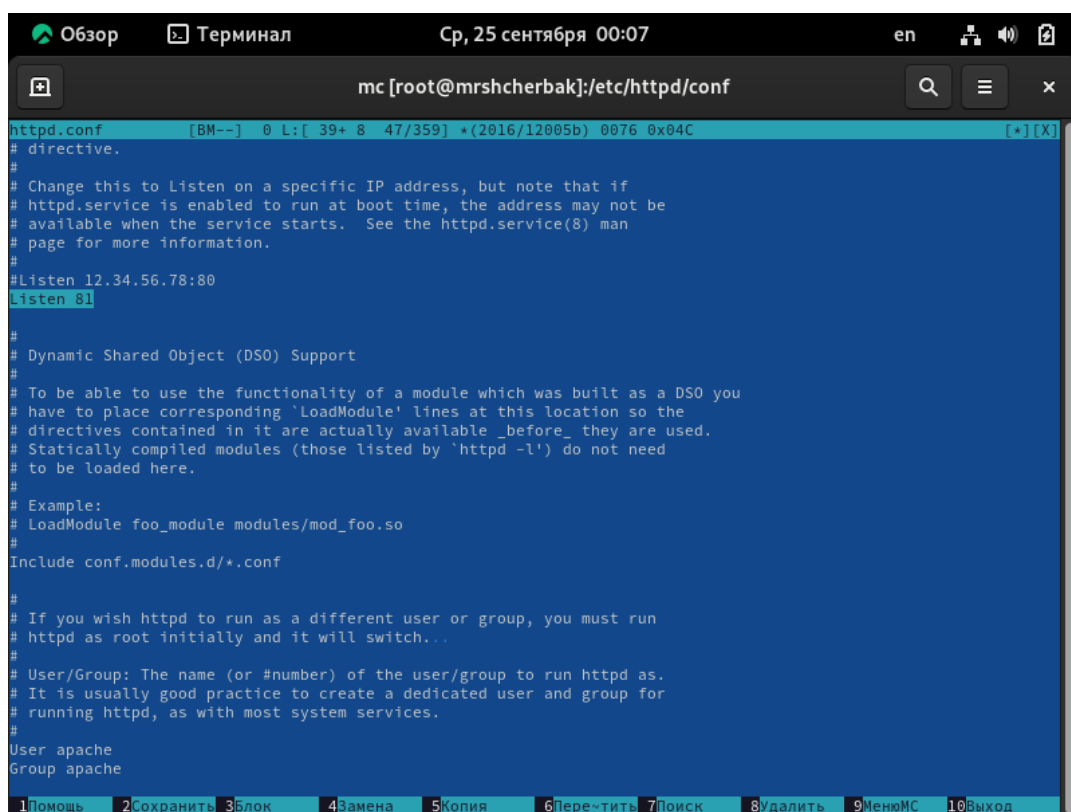


Рис. 12: log-файлы

12. Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81 (рис.13).



```
httpd.conf [BM--] 0 L:[ 39+ 8 47/359] *(2016/12005b) 0076 0x04C [*][X]
# directive.
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#Listen 12.34.56.78:80
Listen 81
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/*.conf
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch...
#
# User/Group: The name (or #number) of the user/group to run httpd as.
# It is usually good practice to create a dedicated user and group for
# running httpd, as with most system services.
#
User apache
Group apache
```

Рис. 13: Замена порта в файле

13. Выполните перезапуск веб-сервера Apache. Сбоя нет. Проанализировала лог-файлы: `tail -nl /var/log/messages` (рис.14). Просмотрела файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` (рис.15 - рис.16).

```
[root@mrshcherbak conf]# tail -n15 /var/log/messages
Sep 25 00:07:35 mrshcherbak systemd[1]: Started SETroubleshoot daemon for processing new SELinux denial logs.
Sep 25 00:07:35 mrshcherbak setroubleshoot[43691]: failed to retrieve rpm info for path '/var/www/html/test.html'
Sep 25 00:07:35 mrshcherbak systemd[1]: Started dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@4.service.
Sep 25 00:07:37 mrshcherbak setroubleshoot[43691]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/
www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l af7e3db7-3cc7-4ace-830a-07bcb3f9c97d
Sep 25 00:07:38 mrshcherbak setroubleshoot[43691]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/
www/html/test.html.#012#012***** Модуль restorecon предлагает (точность 92.2) *****#012#01
2Если вы хотите исправить метку.$TARGET3нак _PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете з
апустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для доступа к род
ительскому каталогу, и в этом случае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#
012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Модуль public_content предлагает (точность 7.83)
*****#012#012Если вы хотите лечить test.html как общедоступный контент#012То необходимо изменит
ь метку test.html с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t public_cont
ent_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Модуль catchall предл
агает (точность 1.41) *****#012#012Если вы считаете, что httpd должно быть разрешено geta
ttr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ
, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -
c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Sep 25 00:07:38 mrshcherbak setroubleshoot[43691]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/
www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l af7e3db7-3cc7-4ace-830a-07bcb3f9c97d
Sep 25 00:07:38 mrshcherbak setroubleshoot[43691]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/
www/html/test.html.#012#012***** Модуль restorecon предлагает (точность 92.2) *****#012#01
2Если вы хотите исправить метку.$TARGET3нак _PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете з
апустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для доступа к род
ительскому каталогу, и в этом случае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#
012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Модуль public_content предлагает (точность 7.83)
*****#012#012Если вы хотите лечить test.html как общедоступный контент#012То необходимо изменит
ь метку test.html с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t public_cont
ent_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Модуль catchall предл
агает (точность 1.41) *****#012#012Если вы считаете, что httpd должно быть разрешено geta
ttr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ
, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, выполнив:#012# ausearch -
c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Sep 25 00:07:40 mrshcherbak setroubleshoot[43691]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/
www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l af7e3db7-3cc7-4ace-830a-07bcb3f9c97d
```

Рис. 14: /var/log/messages

```
mc [root@mrshcherbak]:/var/log/httpd

/var/log/httpd/access_log 1593/1593 100%
127.0.0.1 - - [24/Sep/2024:23:50:26 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [24/Sep/2024:23:50:27 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [24/Sep/2024:23:56:19 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [24/Sep/2024:23:56:22 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [24/Sep/2024:23:57:29 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [24/Sep/2024:23:58:08 +0300] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [25/Sep/2024:00:02:02 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [25/Sep/2024:00:02:02 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [25/Sep/2024:00:07:34 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [25/Sep/2024:00:07:40 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"

1Помощь 2Разверн 3Выход 4Нех 5Перейти 6 7Поиск 8Исходный 9Формат 10Выход
```

Рис. 15: /var/log/http/access_log

```
mc [root@mrshcherbak]:/var/log/httpd
/var/log/httpd/error_log 2417/2417 100%
[Tue Sep 24 23:31:44.231649 2024] [core:notice] [pid 33537:tid 33537] SELinux policy enabled; httpd running as c
ontext system_u:system_r:httpd_t:s0
[Tue Sep 24 23:31:44.234406 2024] [suexec:notice] [pid 33537:tid 33537] AH01232: suEXEC mechanism enabled (wrapp
er: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using fe80::a00:27ff:feba
:df27%enp0s3. Set the 'ServerName' directive globally to suppress this message
[Tue Sep 24 23:31:44.310195 2024] [lbmethod_heartbeat:notice] [pid 33537:tid 33537] AH02282: No slotmem from mod
_heartbeat
[Tue Sep 24 23:31:44.325925 2024] [mpm_event:notice] [pid 33537:tid 33537] AH00489: Apache/2.4.57 (Rocky Linux)
configured -- resuming normal operations
[Tue Sep 24 23:31:44.325953 2024] [core:notice] [pid 33537:tid 33537] AH00094: Command line: '/usr/sbin/httpd -D
FOREGROUND'
[Tue Sep 24 23:50:26.566729 2024] [core:error] [pid 33638:tid 33817] (13)Permission denied: [client 127.0.0.1:45
582] AH00132: file permissions deny server access: /var/www/html/test.html
[Tue Sep 24 23:56:19.721232 2024] [core:error] [pid 33638:tid 33824] (13)Permission denied: [client 127.0.0.1:56
034] AH00132: file permissions deny server access: /var/www/html/test.html
[Tue Sep 24 23:56:22.005466 2024] [core:error] [pid 33638:tid 33816] (13)Permission denied: [client 127.0.0.1:56
034] AH00132: file permissions deny server access: /var/www/html/test.html
[Tue Sep 24 23:57:29.880447 2024] [core:error] [pid 33638:tid 33827] (13)Permission denied: [client 127.0.0.1:57
170] AH00132: file permissions deny server access: /var/www/html/test.html
[Wed Sep 25 00:02:02.259887 2024] [core:error] [pid 33638:tid 33834] (13)Permission denied: [client 127.0.0.1:41
636] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path
[Wed Sep 25 00:07:34.189231 2024] [core:error] [pid 33638:tid 33838] (13)Permission denied: [client 127.0.0.1:33
992] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path
[Wed Sep 25 00:07:40.134795 2024] [core:error] [pid 33638:tid 33841] (13)Permission denied: [client 127.0.0.1:33
998] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions
are missing on a component of the path
```

Рис. 16: /var/log/httpd/error_log

14. Выполнила команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверила список портов командой `semanage port -l | grep http_port_t`. Убедилась, что порт 81 появился в списке. Попробовала запустить веб-сервер Apache ещё раз. Порт 81 был в списке до этого, поэтому сбоя не было. Вернула 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 попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Увидела содержимое файла — слово «test» (рис.17).

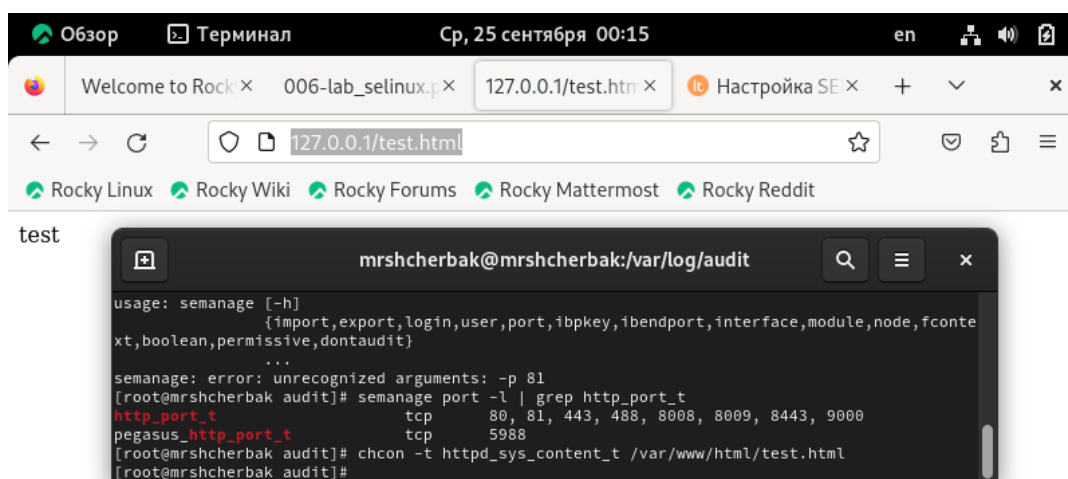


Рис. 17: Semanage и запуск веб-сервера

15. Исправила обратно конфигурационный файл apache, вернув Listen 80. Удалила привязку http_port_t к 81 порту: semanage port -d -t http_port_t -p tcp 81. Удалила файл /var/www/html/test.html (рис.18).



Рис. 18: Удаление файла

Вывод

Таким образом, в ходе ЛР№6 я развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.

Библиография

1. Методические материалы курса.
2. Linux Kernel Security [Электронный ресурс]: URL: <http://www.cyberciti.biz/tips/selinux-vs-apparmor-vs-grsecurity.html> (дата обращения 24.09.2024)
3. Security-Enhanced Linux [Электронный ресурс]: Официальный сайт SELinux. URL: <http://www.nsa.gov/research/selinux/index.shtml> (дата обращения 24.09.2024)