

# **Информационная безопасность. Лабораторная работа #6.**

**Мандатное разграничение прав в Linux**

Хохлачева Яна

# Содержание

0.1	Цель работы . . . . .	3
<b>1</b>	<b>Создание программы</b>	<b>4</b>
1.1	Вывод . . . . .	15

# Список иллюстраций

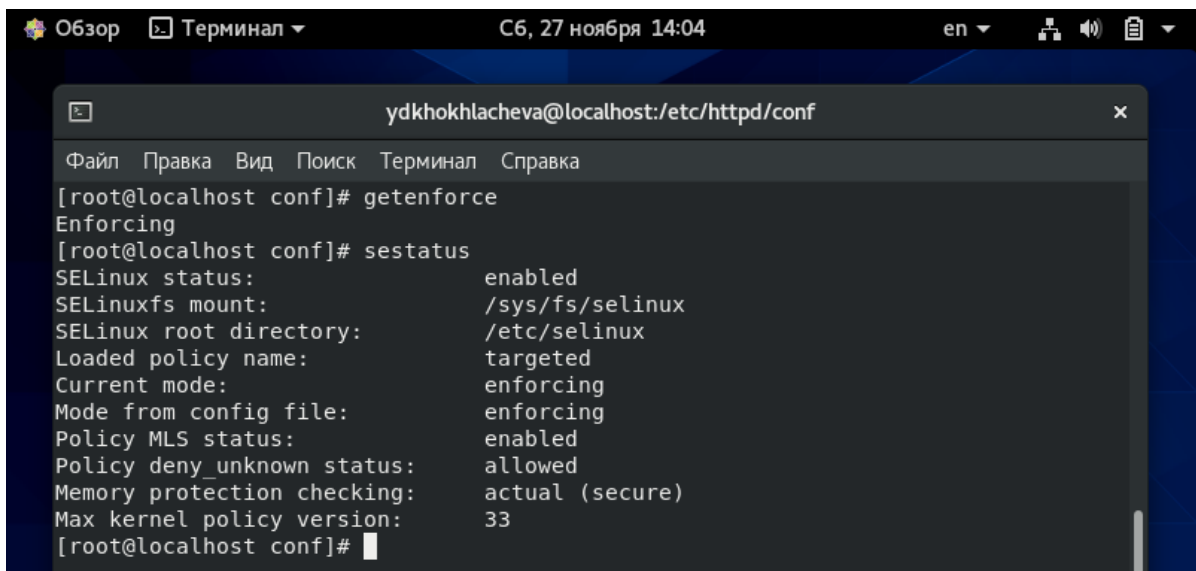
1.1	Проверка SELinux . . . . .	4
1.2	Запуск Apache . . . . .	5
1.3	Статистика по политикеSELinux . . . . .	6
1.4	Файлы в директории html . . . . .	7
1.5	127.0.0.1/test.html . . . . .	8
1.6	Контекст . . . . .	9
1.7	Изменение контекста файла . . . . .	10
1.8	Потерянный доступ . . . . .	10
1.9	Права пользователей . . . . .	11
1.10	Изменение прослушивания порта . . . . .	12
1.11	Изменение списка портов . . . . .	13
1.12	Возвращение контекста . . . . .	14
1.13	Повторное обращение к test.html . . . . .	14
1.14	Удаление файла test.html . . . . .	15

## 0.1 Цель работы

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

# 1 Создание программы

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

A screenshot of a terminal window titled "ydkhokhlacheva@localhost:/etc/httpd/conf". The terminal shows the output of the commands "getenforce" and "sestatus". The "getenforce" command returns "Enforcing". The "sestatus" command returns a detailed status report for SELinux, including its status (enabled), mount point (/sys/fs/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)), and max kernel policy version (33).

```
ydkhokhlacheva@localhost:/etc/httpd/conf
[root@localhost conf]# getenforce
Enforcing
[root@localhost 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
[root@localhost conf]#
```

Рис. 1.1: Проверка SELinux

2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: **service httpd status** или **/etc/rc.d/init.d/httpd status**

Если не работает, запустите его так же, но с параметром **start**.

The screenshot shows a terminal window titled 'ydkhokhlacheva@localhost:/home/ydkhokhlacheva'. The terminal output is as follows:

```
[root@localhost ydkhokhlacheva]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@localhost ydkhokhlacheva]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0  root      4320  0.1  0.3 273832 11168 ?
Ss   14:06   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  4324  0.0  0.2 289836  8216 ?
S    14:06   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  4325  0.0  0.4 1478772 14040 ?
Sl   14:06   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  4327  0.0  0.3 1347644 11992 ?
Sl   14:06   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  4329  0.0  0.3 1347644 11992 ?
Sl   14:06   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4562 0.0  0.0 221928
1140 pts/0 R+ 14:07   0:00 grep --color=auto httpd
[root@localhost ydkhokhlacheva]# sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

  -v Verbose check of process and file contexts.
  -b Display current state of booleans.

Without options, show SELinux status.
```

Рис. 1.2: Запуск Apache

3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду **ps auxZ | grep httpd**
  4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды **sestatus -bigrep httpd**
- Обратите внимание, что многие из них находятся в положении «off».
5. Посмотрите статистику по политике с помощью команды **seinfo**, также определите множество пользователей, ролей, типов.

The screenshot shows a terminal window titled "ydkhokhlacheva@localhost:/home/ydkhokhlacheva". The terminal displays SELinux statistics in two columns:

Category	Count	Category	Count
Users:	8	Roles:	14
Booleans:	337	Cond. Expr.:	383
Allow:	110945	Neverallow:	0
Auditallow:	163	Dontaudit:	10255
Type_trans:	244757	Type_change:	87
Type_member:	35	Range_trans:	6015
Role_allow:	37	Role_trans:	422
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:	640
Netifcon:	0	Nodecon:	0

Below the statistics, the terminal shows the execution of the command `ls -lZ /var/www`, resulting in the following output:

```
[root@localhost ydkhokhlacheva]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07:58
cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 12 07:58
html
[root@localhost ydkhokhlacheva]# ls -lZ /var/www/html
итого 0
[root@localhost ydkhokhlacheva]#
```

Рис. 1.3: Статистика по политикеSELinux

6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`
7. Определите тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`

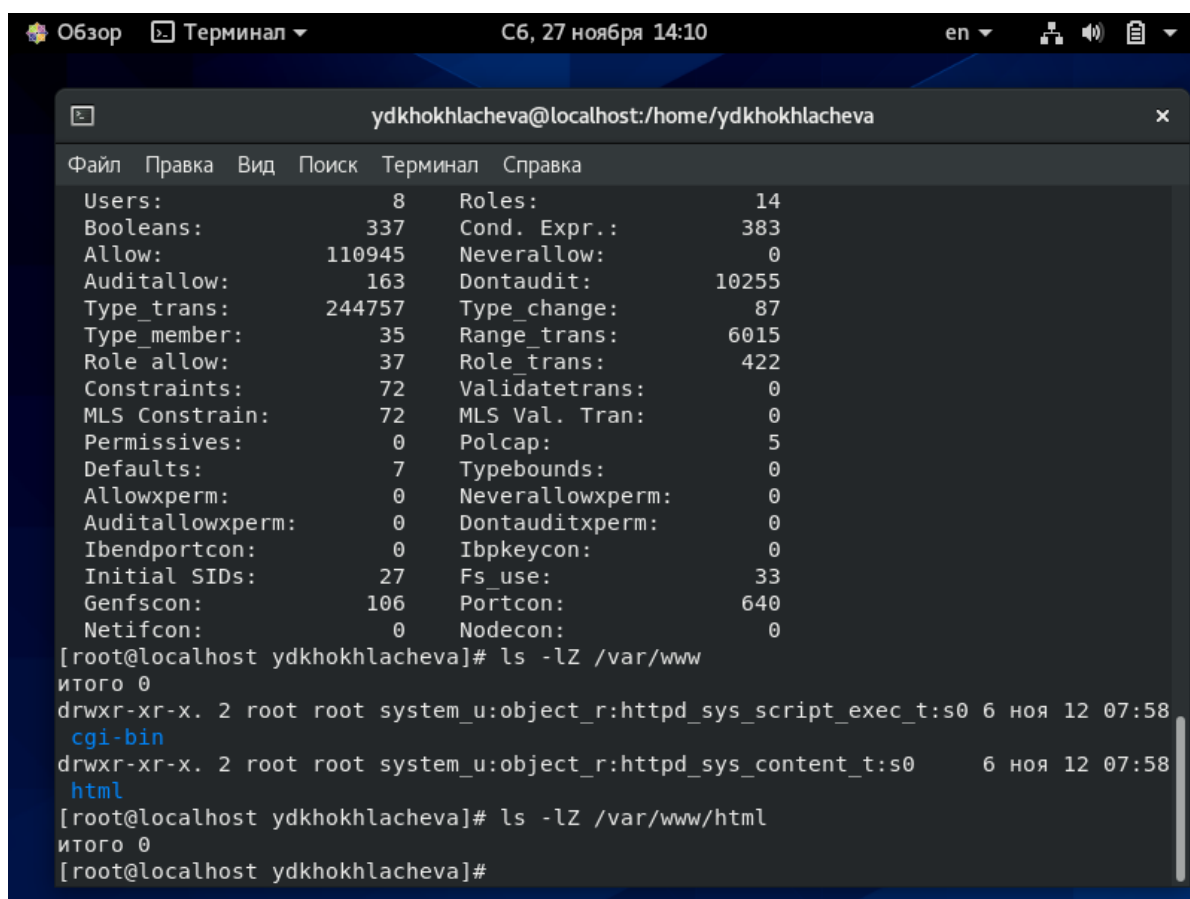


Рис. 1.4: Файлы в директории html

8. Определите круг пользователей, которым разрешено создание файлов в директории **/var/www/html**.
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>

```

10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваивае-

мый по умолчанию вновь созданным файлам в директории `/var/www/html`.

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

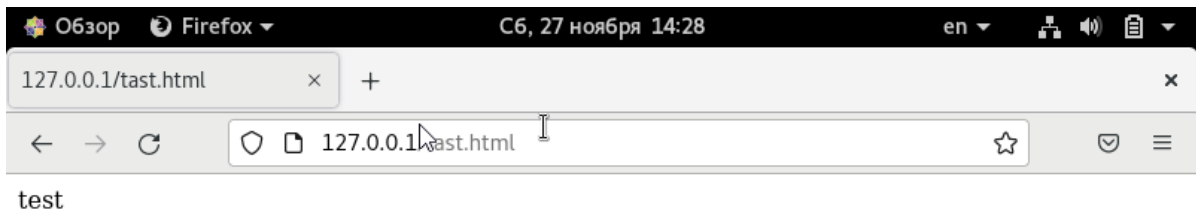
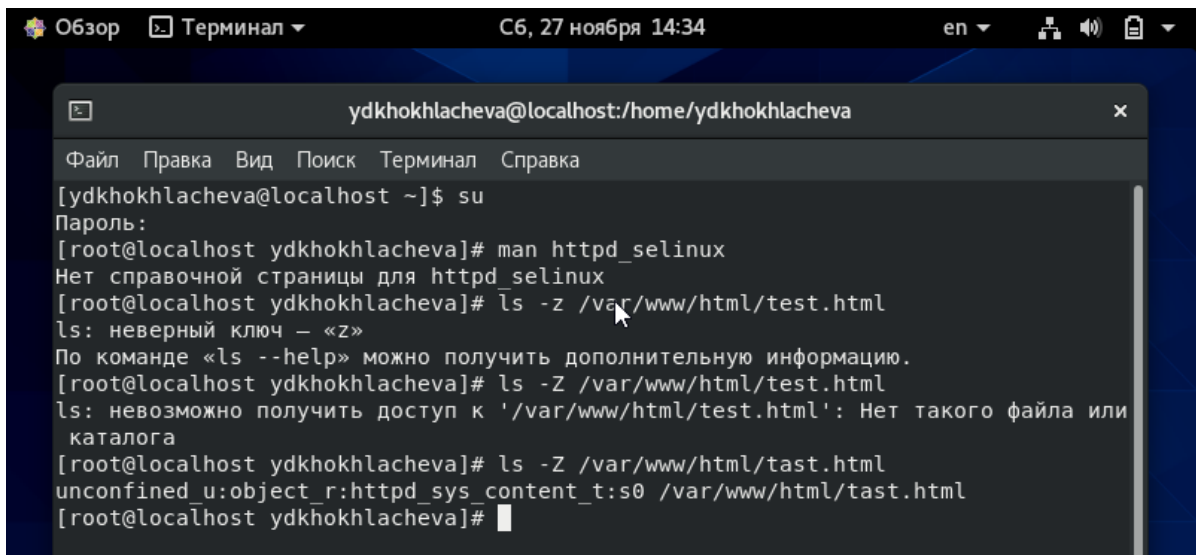


Рис. 1.5: 127.0.0.1/test.html

12. Изучите справку **man httpd\_selinux** и выясните, какие контексты файлов определены для **httpd**. Сопоставьте их с типом файла **test.html**. Проверить контекст файла можно командой **\*\* ls -Z /var/www/html/test.html** **Рассмотрим полученный контекст детально. Обратите внимание, что так как по умолчанию пользователи CentOS являются свободными от типа (unconfined в переводе с англ. означает свободный), созданному нами файлу test.html\*\*** был сопоставлен SELinux, пользователь **unconfined\_u**. Это первая часть контекста. Далее политика ролевого разделения доступа RBAC используется процессами, но не файлами, поэтому роли не имеют никакого значения для файлов. Роль **object\_r** используется по умолчанию для файлов на «постоянных» носителях и на сетевых файловых системах. (В директории **/proc** файлы, относящиеся к процессам, могут иметь роль **system\_r**. Если активна политика MLS, то могут использоваться и другие роли, например, **secadm\_r**. Данный случай мы рассматривать не будем, как и предназначение **:s0**). Тип **httpd\_sys\_content\_t** позволяет процессу **httpd** получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.





The screenshot shows a terminal window titled "ydkhokhlacheva@localhost:/home/ydkhokhlacheva". The user is in the root shell (su). The commands and output are as follows:

```
[ydkhokhlacheva@localhost ~]$ su
Пароль:
[root@localhost ydkhokhlacheva]# man httpd_selinux
Нет справочной страницы для httpd_selinux
[root@localhost ydkhokhlacheva]# ls -z /var/www/html/test.html
ls: неверный ключ - «z»
По команде «ls --help» можно получить дополнительную информацию.
[root@localhost ydkhokhlacheva]# ls -Z /var/www/html/test.html
ls: невозможно получить доступ к '/var/www/html/test.html': Нет такого файла или каталога
[root@localhost ydkhokhlacheva]# ls -Z /var/www/html/tast.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/tast.html
[root@localhost ydkhokhlacheva]#
```

Рис. 1.6: Контекст

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`: `chcon -t samba_share_t /var/www/html/test.html ls -Z /var/www/html/test.html`

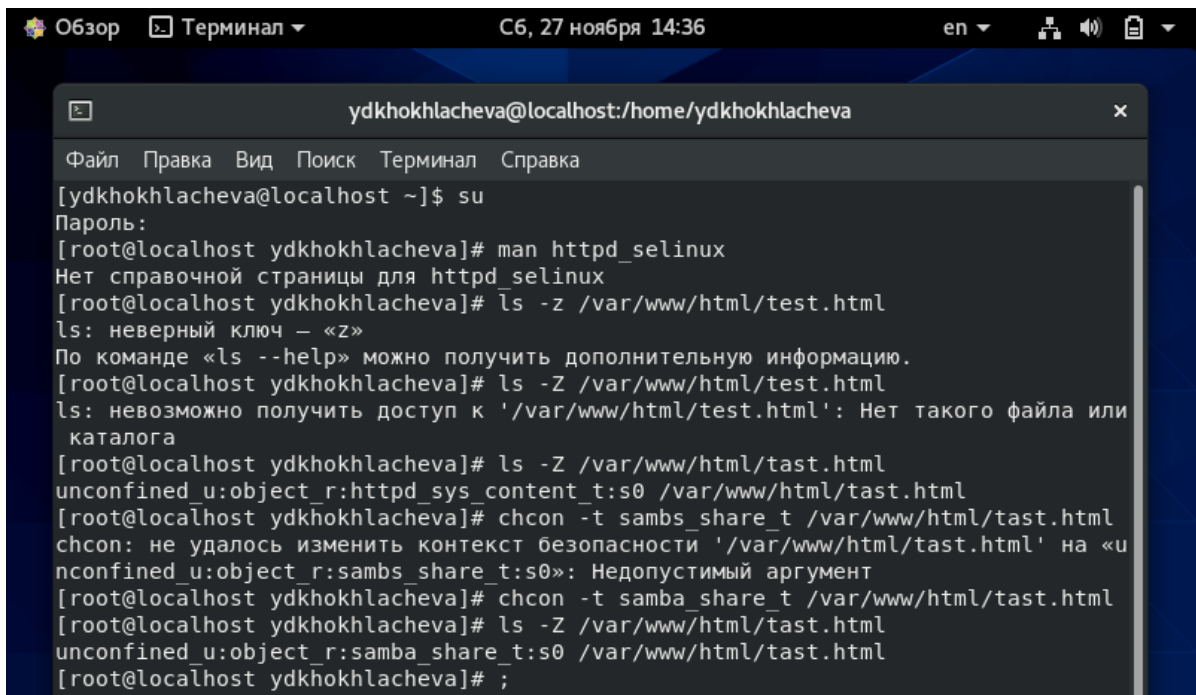


Рис. 1.7: Изменение контекста файла

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: **Forbidden You don't have permission to access /test.html on this server.**

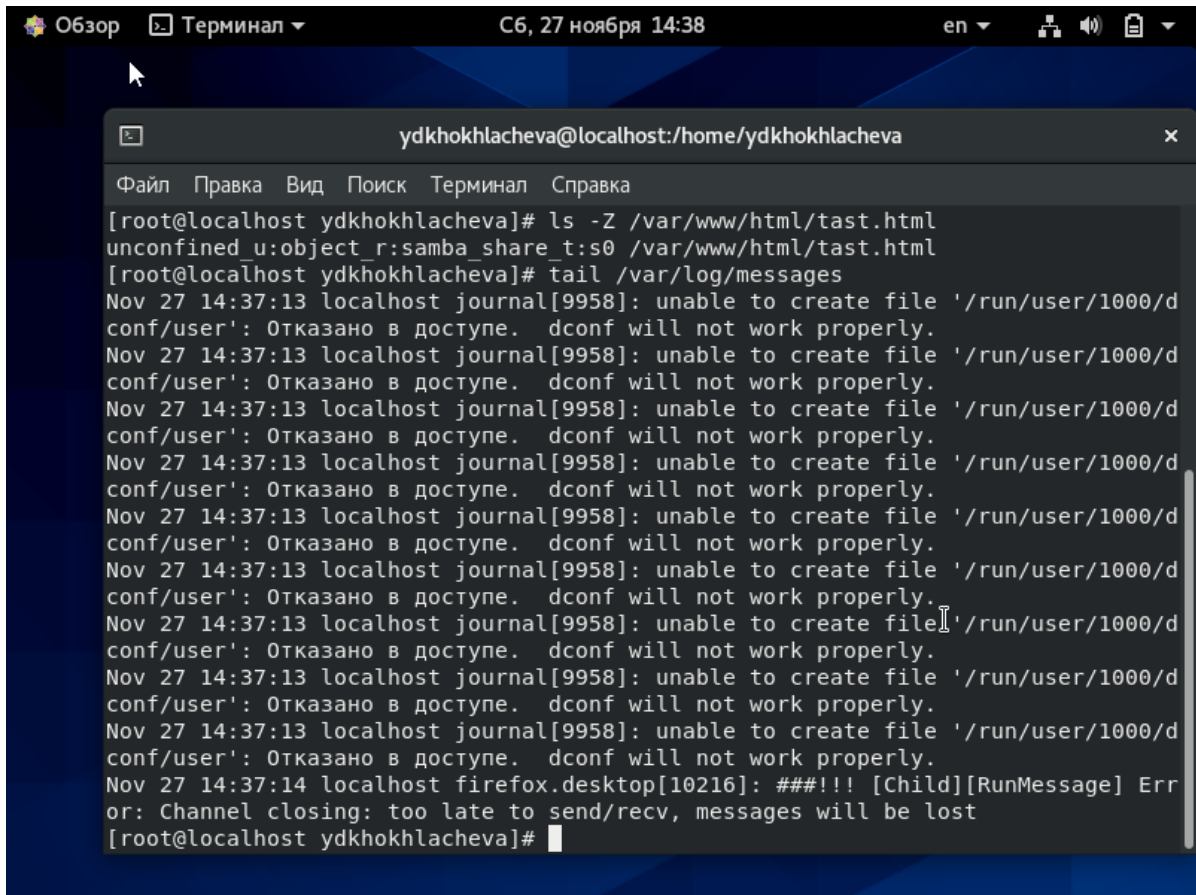


Рис. 1.8: Потерянный доступ

15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа

позволяют читать этот файл любому пользователю? `ls -l /var/www/html/test.html`

Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail /var/log/messages` Если в системе окажутся запущенными процессы `setroubleshootd` и `audtd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно.



The screenshot shows a terminal window titled "ydkhokhlacheva@localhost:/home/ydkhokhlacheva". The terminal output is as follows:

```
[root@localhost ydkhokhlacheva]# ls -Z /var/www/html/tast.html
unconfined u:object_r:samba_share_t:s0 /var/www/html/tast.html
[root@localhost ydkhokhlacheva]# tail /var/log/messages
Nov 27 14:37:13 localhost journal[9958]: unable to create file '/run/user/1000/d
conf/user': Отказано в доступе. dconf will not work properly.
Nov 27 14:37:13 localhost journal[9958]: unable to create file '/run/user/1000/d
conf/user': Отказано в доступе. dconf will not work properly.
Nov 27 14:37:13 localhost journal[9958]: unable to create file '/run/user/1000/d
conf/user': Отказано в доступе. dconf will not work properly.
Nov 27 14:37:13 localhost journal[9958]: unable to create file '/run/user/1000/d
conf/user': Отказано в доступе. dconf will not work properly.
Nov 27 14:37:13 localhost journal[9958]: unable to create file '/run/user/1000/d
conf/user': Отказано в доступе. dconf will not work properly.
Nov 27 14:37:13 localhost journal[9958]: unable to create file '/run/user/1000/d
conf/user': Отказано в доступе. dconf will not work properly.
Nov 27 14:37:13 localhost journal[9958]: unable to create file '/run/user/1000/d
conf/user': Отказано в доступе. dconf will not work properly.
Nov 27 14:37:13 localhost journal[9958]: unable to create file '/run/user/1000/d
conf/user': Отказано в доступе. dconf will not work properly.
Nov 27 14:37:13 localhost journal[9958]: unable to create file '/run/user/1000/d
conf/user': Отказано в доступе. dconf will not work properly.
Nov 27 14:37:13 localhost journal[9958]: unable to create file '/run/user/1000/d
conf/user': Отказано в доступе. dconf will not work properly.
Nov 27 14:37:14 localhost firefox.desktop[10216]: ###!!! [Child][RunMessage] Err
or: Channel closing: too late to send/recvd, messages will be lost
[root@localhost ydkhokhlacheva]#
```

Рис. 1.9: Права пользователей

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**.

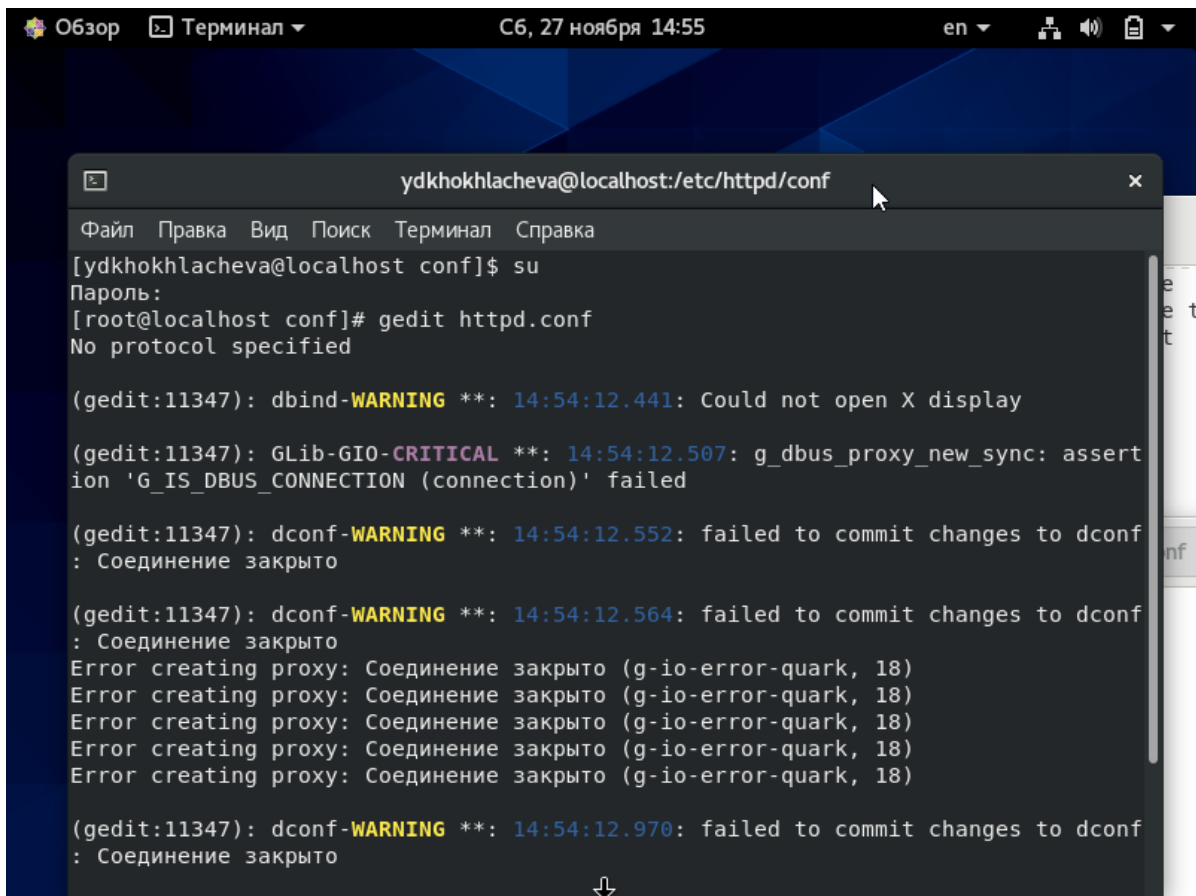


Рис. 1.10: Изменение прослушивания порта

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

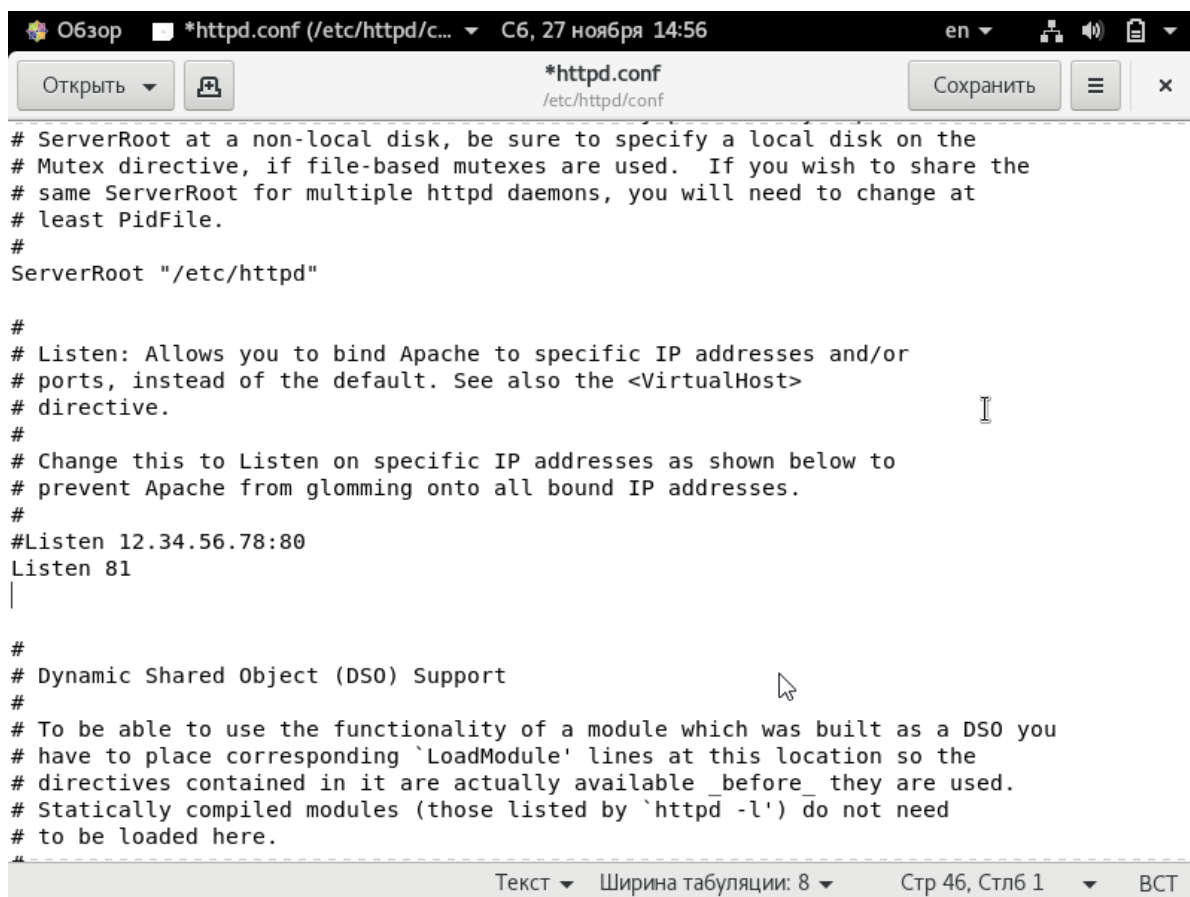


Рис. 1.11: Изменение списка портов

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

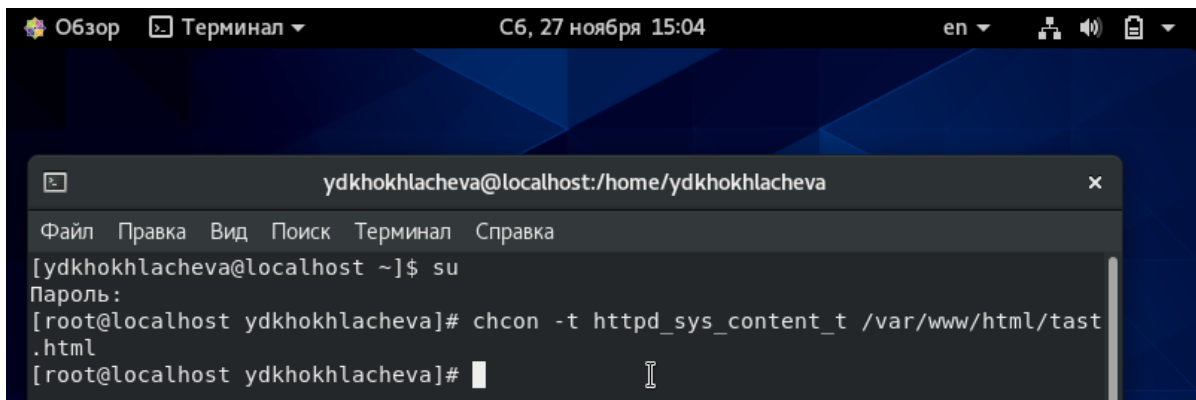


Рис. 1.12: Возвращение контекста

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».

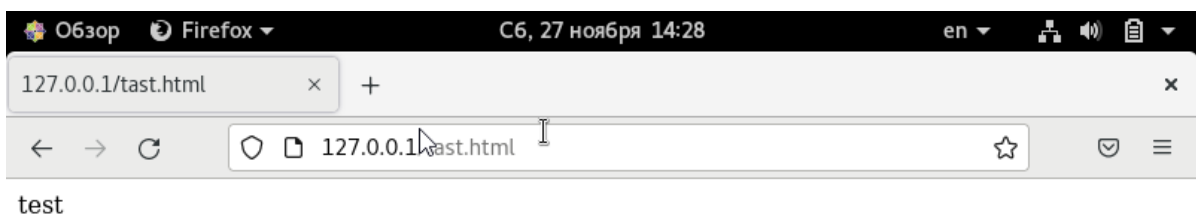


Рис. 1.13: Повторное обращение к test.html

22. Исправьте обратно конфигурационный файл `apache`, вернув **Listen 80**.
23. Удалите привязку `http_port_t` к **81** порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.
24. Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html`

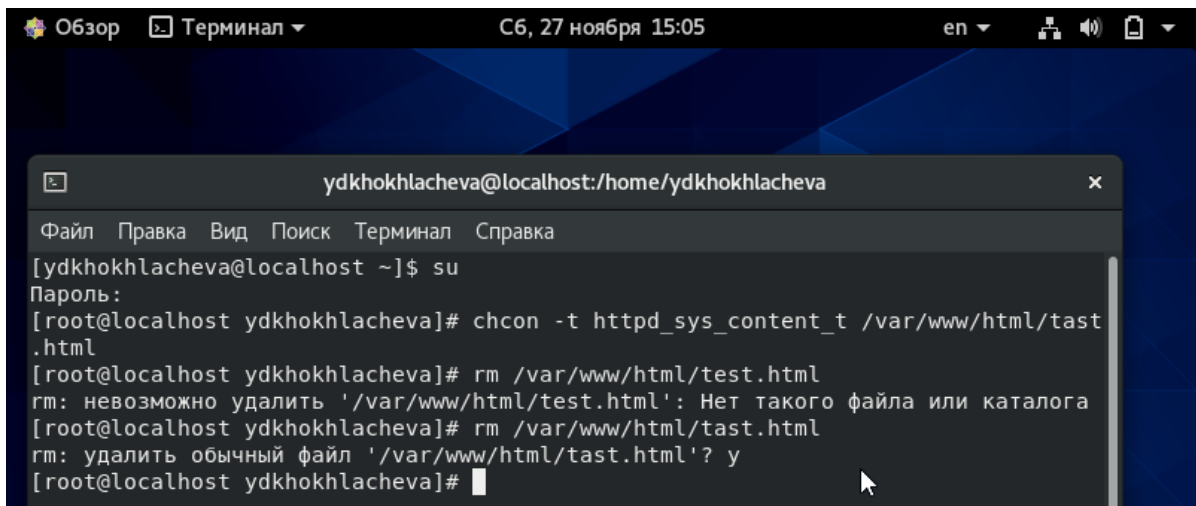


Рис. 1.14: Удаление файла test.html

## 1.1 Вывод

- Развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux.
- Проверила работу SELinux на практике совместно с веб-сервером Apache.