

# **Лабораторная работа №6**

**Дисциплина: Основы информационной безопасности**

Коновалова Татьяна Борисовна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Теоретические данные</b>	<b>6</b>
<b>3</b>	<b>Задание</b>	<b>8</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>9</b>
<b>5</b>	<b>Выводы</b>	<b>17</b>
<b>6</b>	<b>Библиография</b>	<b>18</b>

## Список иллюстраций

4.1	getenforce и sestatus . . . . .	9
4.2	Проверка работы сервера . . . . .	10
4.3	Контекст безопасности Apache . . . . .	10
4.4	Состояние переключателей . . . . .	11
4.5	Статистика seinfo . . . . .	11
4.6	Данные директорий /var/www и /var/www/html . . . . .	12
4.7	Файл test.html . . . . .	12
4.8	Обращение к файлу через веб-сервер . . . . .	12
4.9	Изменение контекста файла . . . . .	13
4.10	Ошибка доступа при открытии файла через веб-сервер . . . . .	13
4.11	Ошибки в log-файлах . . . . .	14
4.12	Прослушивание 81 порта . . . . .	14
4.13	Перезапуск сервера . . . . .	15
4.14	Установка порта . . . . .	15
4.15	Возвращаем файлу исходный контекст . . . . .	15
4.16	Повторный просмотр файла в веб-браузере . . . . .	15
4.17	Удаление порта . . . . .	16
4.18	Удаление файла . . . . .	16

## **Список таблиц**

# 1 Цель работы

Цель лабораторной работы — Получить практические навыки администрирования в ОС Linux и ознакомиться с технологией SELinux совместно с веб-сервером Apache.

## 2 Теоретические данные

SELinux, или Security Enhanced Linux, — это продвинутый механизм управления доступом, разработанный Агентством национальной безопасности (АНБ) США для предотвращения злонамеренных вторжений. Он реализует мандатную модель управления доступом (MAC — Mandatory Access control) в дополнение к уже существующей в Linux дискреционной модели (DAC — Discretionary Access Control), то есть разрешениям на чтение, запись, выполнение.

У SELinux есть три режима работы:

- Enforcing — ограничение доступа в соответствии с политикой. Запрещено все, что не разрешено в явном виде. Режим по умолчанию.
- Permissive — ведёт лог действий, нарушающих политику, которые в режиме enforcing были бы запрещены, но не запрещает сами действия.
- Disabled — полное отключение SELinux.

В основе структуры безопасности SELinux лежат политики. Политика — это набор правил, определяющих ограничения и права доступа для всего, что есть в системе. Под “всем” в данном случае понимаются пользователи, роли, процессы и файлы. Политика определяет связь этих категорий друг с другом. |

Apache — это свободное программное обеспечение, с помощью которого можно создать веб-сервер. Несмотря на то, что Apache чаще всего называют сервером (более того, его официальное название — Apache HTTP Server) — это всё-таки программа, которую устанавливают на сервер, чтобы добиться определённых результатов.

Для чего нужен Apache сервер:

- чтобы открывать динамические PHP-страницы,
- для распределения поступающей на сервер нагрузки,
- для обеспечения отказоустойчивости сервера,
- чтобы потренироваться в настройке сервера и запуске PHP-скриптов.

Apache является кроссплатформенным ПО и поддерживает такие операционные системы, как Linux, BSD, MacOS, Microsoft, BeOS и другие.

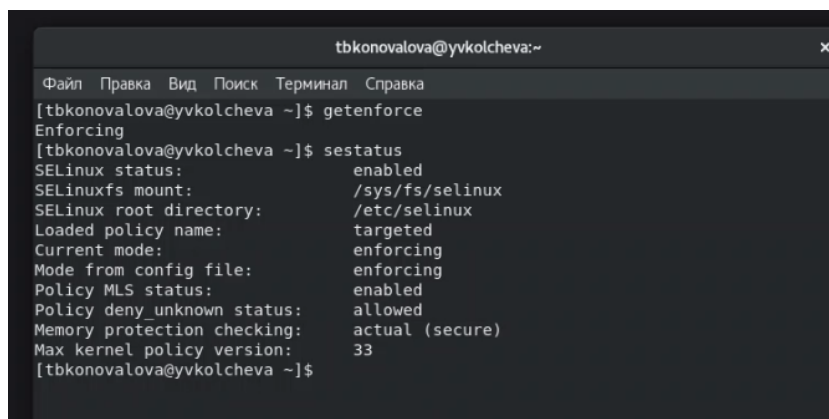
## 3 Задание

1. Найти веб-сервер Apache в списке процессов, определить его контекст безопасности и занести эту информацию в отчёт. 2. Посмотреть текущее состояние переключателей SELinux для Apache; 3. Изучить справку `man httpd_selinux` 4. Определить тип файлов, находящихся в директории `/var/www/html`.



## 4 Выполнение лабораторной работы

1. Вошла в систему под своей учетной записью и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команды `getenforce` и `sestatus` (рис. [4.1]).

A screenshot of a terminal window titled 'tbkonovalova@yvkolcheva:~'. The terminal shows the output of the 'getenforce' and 'sestatus' commands. 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).

```
tbkonovalova@yvkolcheva:~  
[tbkonovalova@yvkolcheva ~]$ getenforce  
Enforcing  
[tbkonovalova@yvkolcheva ~]$ 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  
[tbkonovalova@yvkolcheva ~]$
```

Рис. 4.1: `getenforce` и `sestatus`

2. Убедилась, что сервер работает с помощью команды `service httpd status` (рис. [4.2]).

```
Выполнено!
[root@yvkolcheva tbkonovalova]# systemctl start httpd
[root@yvkolcheva tbkonovalova]# 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; vendor preset: disabled)
   Active: active (running) since Mon 2023-10-09 12:46:28 MSK; 5s ago
     Docs: man:httpd.service(8)
  Main PID: 16417 (httpd)
    Status: "Started, listening on: port 80"
    Tasks: 213 (limit: 11025)
   Memory: 20.7M
    CGroup: /system.slice/httpd.service
            └─16417 /usr/sbin/httpd -DFOREGROUND
              └─21577 /usr/sbin/httpd -DFOREGROUND
                └─21578 /usr/sbin/httpd -DFOREGROUND
                  └─21579 /usr/sbin/httpd -DFOREGROUND
                    └─21580 /usr/sbin/httpd -DFOREGROUND

окт 09 12:46:22 yvkolcheva.myquest.virtualbox.org systemd[1]: Starting The Apache HTTP Server...
окт 09 12:46:28 yvkolcheva.myquest.virtualbox.org systemd[1]: Started The Apache HTTP Server.
окт 09 12:46:31 yvkolcheva.myquest.virtualbox.org httpd[16417]: Server configured, listening on: port 80
lines 1-18/18 (END)
```

Рис. 4.2: Проверка работы сервера

3.С помощью команды `ps -eZ` нашла, что контекст безопасности Apache — `httpd_t` (рис. [4.3]).

```
[tbkonovalova@yvkolcheva ~]$ ps auxZ | grep httpd
system u:system r:httpd t:s0 root 16417 0.0 0.6 265100 11368 ? Ss 12:46 0:00 /usr
/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 21577 0.0 0.4 269800 8580 ? S 12:46 0:00 /usr
/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 21578 0.0 0.6 1458720 12308 ? Sl 12:46 0:00 /usr
/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 21579 0.0 0.5 1327592 10256 ? Sl 12:46 0:00 /usr
/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 21580 0.0 0.5 1327592 10256 ? Sl 12:46 0:00 /usr
/sbin/httpd -DFOREGROUND
unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 root 23238 0.0 0.4 291984 7796 pts/1 S+ 12:46
0:00 /bin/systemctl status httpd.service
unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 tbkonov+ 49865 0.0 0.0 221940 1188 pts/0 R+ 12:4
8 0:00 grep --color=auto httpd
[tbkonovalova@yvkolcheva ~]$
```

Рис. 4.3: Контекст безопасности Apache

4.Посмотрела текущее состояние переключателей командой `sestatus -b httpd` (рис. [4.4]).

```
[tbkonovalova@yvkolcheva ~]$ sestatus -bigrep httpd
sestatus: invalid option -- '1'

Usage: sestatus [OPTION]

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

Without options, show SELinux status.
[tbkonovalova@yvkolcheva ~]$ sestatus -b httpd
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

Policy booleans:
abrt_anon_write                off
abrt_handle_event              off
abrt_upload_watch_anon_write   on
antivirus_can_scan_system      off
antivirus_use_jit              on
auditadm_exec_content          on
authlogin_nsswitch_use_ldap     off
authlogin_radius               off
authlogin_yubikey              off
awstats_purge_apache_log_files off
boinc_execmem                  on
```

Рис. 4.4: Состояние переключателей

5.Посмотрела статистику по политике командой seinfo. Узнала, что множество пользователей — 8, ролей — 14, типов — 5010 (рис. [4.5]).

```
[tbkonovalova@yvkolcheva ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          31 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                  132
Sensitivities:            1
Types:                   5010
Users:                    8
Booleans:                 342
Allow:                   115062
Auditallow:              168
Type_trans:              257610
Type_member:              35
Role_allow:               38
Constraints:              72
MLS Constrain:           72
Permissives:              0
Defaults:                 7
Allowxperm:               0
Auditallowxperm:         0
Ibendportcon:            0
Initial SIDs:             27
Genfscon:                 107
Netifcon:                 0
Permissions:              464
Categories:              1024
Attributes:               257
Roles:                    14
Cond. Expr.:              390
Neverallow:               0
Dontaudit:                10439
Type_change:              87
Range_trans:              5989
Role_trans:               422
Validatetrans:            0
MLS Val. Tran:            0
Polcap:                   5
Typebounds:               0
Neverallowxperm:         0
Dontauditxperm:          0
Ibpkeycon:                0
Fs_use:                   34
Portcon:                  649
Nodecon:                  0
```

Рис. 4.5: Статистика seinfo

6.Определила тип файлов и круг пользователей с правой на создание и поддиректорий в директориях /var/www и /var/www/html командой ls -lZ (рис. [4.6]).

```

[tbkonovalova@yvkolcheva ~]$ ls -lZ /var/www
итого 8
drwxr-xr-x. 2 root root system u:object r:httpd_sys_script_exec_t:s0 4096 сен 23 02:22 cgi-bin
drwxr-xr-x. 2 root root system u:object r:httpd_sys_content_t:s0 4096 сен 23 02:22 html
[tbkonovalova@yvkolcheva ~]$ ls -lZ /var/www/html
итого 0
[tbkonovalova@yvkolcheva ~]$

```

Рис. 4.6: Данные директорий /var/www и /var/www/html

7. От имени суперпользователя создала файл /var/www/html/test.html (рис. [4.7]).

```

tbkonovalova@yvkolcheva:~
Файл Правка Вид Поиск Терминал Вкладки Справка
tbkonovalova@yvkolcheva:~ x tbkonovalova@yvkolcheva:/hom... x tbkonovalova@yvkolcheva:~ x
[tbkonovalova@yvkolcheva ~]$ su -
Пароль:
Последний вход в систему: Пн окт 9 12:44:25 MSK 2023 на pts/1
[root@yvkolcheva ~]# touch /var/www/html/test.html
[root@yvkolcheva ~]# nano /var/www/html/test.html
[root@yvkolcheva ~]# cat /var/www/html/test.html
[root@yvkolcheva ~]# nano /var/www/html/test.html
[root@yvkolcheva ~]# cat /var/www/html/test.html
[root@yvkolcheva ~]# su - tbkonovalova
Last login: Mon Oct 9 11:26:46 MSK 2023 on tty2
[tbkonovalova@yvkolcheva ~]$ ls -lZ /var/www/html
unconfined u:object r:httpd_sys_content_t:s0 test.html
[tbkonovalova@yvkolcheva ~]$

```

Рис. 4.7: Файл test.html

Обратилась к файлу через веб-сервер, введя в браузер адрес “http://127.0.0.1/test.html”. Файл был успешно отображен (рис. [-#fig:008]).

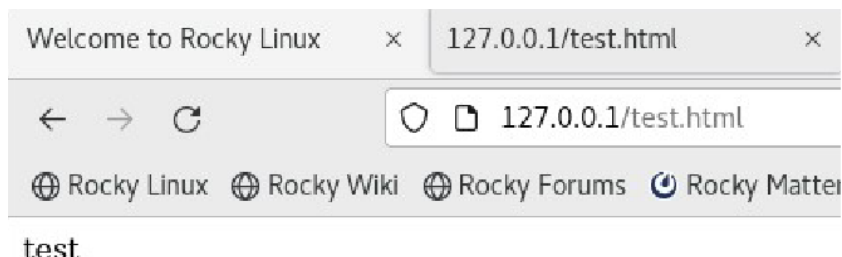


Рис. 4.8: Обращение к файлу через веб-сервер

8. Изучив справку `man httpd_selinux`, выяснила, что для `httpd` определены следующие контексты файлов: `httpd_sys_content_t`, `httpd_sys_script_exec_t`, `httpd_sys_script_ro_t`, `httpd_sys_script_rw_t`, `httpd_sys_script_ra_t`, `httpd_unconfined_script_exec_t`.

Контекст моего файла - `httpd_sys_content_t` (в таком случае содержимое должно быть доступно для всех скриптов `httpd` и для самого демона). Изменила контекст файла на `samba_share_t` командой “`sudo chcon -t samba_share_t /var/www/html/test.html`” . После этого убедилась, что контекст поменялся (рис. [-#fig:009]).

```
[tbkonovalova@yvkolcheva ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[tbkonovalova@yvkolcheva ~]$ chcon -t samba_share_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:samba_share_t:s0': Operation not permitted
[tbkonovalova@yvkolcheva ~]$ su
Password:
[root@yvkolcheva tbkonovalova]# chcon -t samba_share_t /var/www/html/test.html
[root@yvkolcheva tbkonovalova]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@yvkolcheva tbkonovalova]#
```

Рис. 4.9: Изменение контекста файла

9. При повторной попытке открыть файл через веб-браузер я получила ошибку доступа (рис. [4.10]).

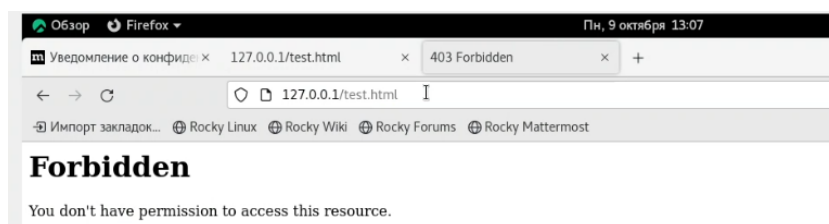


Рис. 4.10: Ошибка доступа при открытии файла через веб-сервер

10. Убедилась, что файл доступен для чтения всем пользователям командой `ls -l`. Далее посмотрела log-файлы веб-сервера Apache командой `tail`, где показаны ошибки (рис. [4.11]).

```
tbkonovalova@yvkolcheva:/hom... x tbkonovalova@yvkolcheva:/hom... x tbkonovalova@yvkolcheva:/hom... x
-rw-r--r-- 1 root root 0 окт 9 12:55 /var/www/html/test.html
[tbkonovalova@yvkolcheva ~]$ tail /var/log/messages
tail: невозможно открыть '/var/log/messages' для чтения: Permission denied
[tbkonovalova@yvkolcheva ~]$ su
Пароль:
[root@yvkolcheva tbkonovalova]# tail /var/log/messages
Oct 9 13:07:57 yvkolcheva dbus-daemon[1910]: [system] Activating service name='org.fedoraproject.Setrou
ubleshootPrivileged' requested by ':1.688' (uid=992 pid=51103 comm="/usr/libexec/platform-python -Es /u
sr/sbin/setroub" label="system u:system r:setroubleshoot t:s0") (using servicehelper)
Oct 9 13:07:59 yvkolcheva dbus-daemon[1910]: [system] Successfully activated service 'org.fedoraprojec
t.SetroubleshootPrivileged'
Oct 9 13:08:02 yvkolcheva setroubleshoot[51103]: SELinux is preventing /usr/sbin/httpd from getattr ac
cess on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l be4c2b20-1ee3-4
d37-96b5-bc93311c0afc
Oct 9 13:08:02 yvkolcheva setroubleshoot[51103]: SELinux is preventing /usr/sbin/httpd from getattr ac
cess on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests
*****#012#012If you want to fix the label. #012/var/www/html/test.html default label
should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stoppe
d due to insufficient permissions to access a parent directory in which case try to change the followin
g command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin publ
ic content (7.83 confidence) suggests *****#012#012If you want to treat test.html as p
ublic content#012Then you need to change the label on test.html to public content t or public content r
w t.#012Do#012# semanage fcontext -a -t public content t '/var/www/html/test.html'#012# restorecon -v '
/var/www/html/test.html'#012#012***** Plugin catchall (1.41 confidence) suggests *****#012#012If
you believe that httpd should be allowed getattr access on the test.html file by defa
ult.#012Then you should report this as a bug.#012You can generate a local policy module to allow this a
ccess.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M
my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 9 13:08:03 yvkolcheva setroubleshoot[51103]: SELinux is preventing /usr/sbin/httpd from getattr ac
cess on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests
*****#012#012If you want to fix the label. #012/var/www/html/test.html default label
should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stoppe
d due to insufficient permissions to access a parent directory in which case try to change the followin
g command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin publ
ic content (7.83 confidence) suggests *****#012#012If you want to treat test.html as p
```

Рис. 4.11: Ошибки в log-файлах

11. Установила веб-сервер Apache на прослушивание TCP-порта 81, изменяя строку Listen в файле /etc/httpd/conf/httpd.conf (рис. [4.12]).

```
tbkonovalova@yvkolcheva:~ x tbkonovalova@yvkolcheva:/hom... x tbkonovalova@yvkolcheva:/hom... x
GNU nano 2.9.8 /etc/httpd/conf/httpd.conf Изменён
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 81
```

Рис. 4.12: Прослушивание 81 порта

12. Перезапустила сервер и увидела данные log-файлов веб-сервера Apache (рис. [4.13]).

```
[root@yvkolcheva tbkonovalova]# systemctl restart httpd
[root@yvkolcheva tbkonovalova]# tail -n1 /var/log/messages
Oct 9 13:41:57 yvkolcheva httpd[52617]: Server configured, listening on: port 81
[root@yvkolcheva tbkonovalova]#
```

Рис. 4.13: Перезапуск сервера

13. Установила для веб-сервера Apache порт TCP-81 и проверила его наличие в списке портов командой `semanage` (рис. [4.14]).

```
[root@yvkolcheva tbkonovalova]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@yvkolcheva tbkonovalova]# semanage -l | grep http_port_t
semanage: error: the following arguments are required: subcommand
[root@yvkolcheva tbkonovalova]# semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@yvkolcheva tbkonovalova]# systemctl restart httpd
[root@yvkolcheva tbkonovalova]#
```

Рис. 4.14: Установка порта

14. Вернула файлу `test.html` контекст `httpd_sys_content_t` и снова успешно просмотрела страницу в веб-браузере (рис. [4.15]) и (рис. [4.16]).

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

Рис. 4.15: Возвращаем файлу исходный контекст

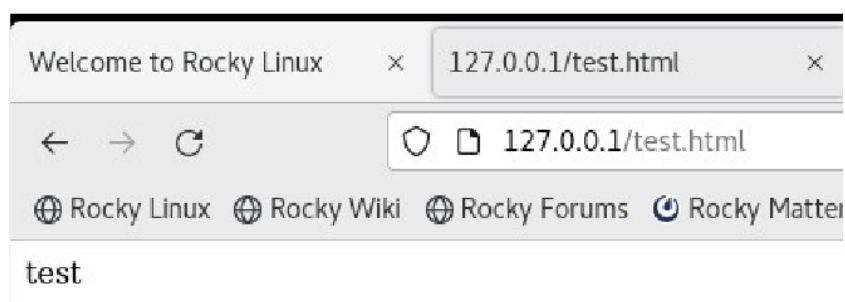


Рис. 4.16: Повторный просмотр файла в веб-браузере

17.Вернула в конфигурационный файл прослушивание порта 80 и удалила порт 81 из списка портов (рис. [4.17]).

```
[root@yvkolcheva tbkonovalova]# nano /etc/httpd/conf/httpd.conf
[root@yvkolcheva tbkonovalova]# semanage port -d -t http_port_t -p tcp 81\
>
^[[AValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@yvkolcheva tbkonovalova]# semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t tcp      5988
[root@yvkolcheva tbkonovalova]# cat /etc/httpd/conf/httpd.conf | grep "Listen"
# Listen: Allows you to bind Apache to specific IP addresses and/or
# Change this to Listen on specific IP addresses as shown below to
#Listen 12.34.56.78:80
Listen 80
[root@yvkolcheva tbkonovalova]#
```

Рис. 4.17: Удаление порта

18.Удалила файл test.html (рис. [4.18]).

```
[root@yvkolcheva tbkonovalova]# rm /var/www/html/test.html
rm: удалить пустой обычный файл '/var/www/html/test.html'? y
[root@yvkolcheva tbkonovalova]# ls /var/www/html
[root@yvkolcheva tbkonovalova]#
```

Рис. 4.18: Удаление файла



## 5 Выводы

Получила практические навыки администрирования в ОС Linux и ознакомилась с технологией SELinux совместно с веб-сервером Apache.

## 6 Библиография

### СПИСОК ЛИТЕРАТУРЫ

- 1.Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: <http://bugtraq.ru/library/books/attack1/index.html>
- 2.Теоретические знания, приведённые в Лабораторной работе №6 - [https://esystem.rudn.ru/pluginfile.php/2090131/mod\\_resource/content/2/006-lab\\_selinux.pdf](https://esystem.rudn.ru/pluginfile.php/2090131/mod_resource/content/2/006-lab_selinux.pdf)
- 3.Запечников С. В. и др. Информационная безопасность открытых систем. Том 1. — М.: Горячая линия -Телеком, 2006.

### СПИСОК ИНТЕРНЕТ-ИСТОЧНИКОВ

- 1.[Электронный ресурс] - доступ: <https://codeby.school/blog/informacionnaya-bezopasnost/razgranichenie-dostupa-v-linux-znakomstvo-s-astra-linux>
- 2.[Электронный ресурс] - доступ: <https://debianinstall.ru/diskretnoe-razgranichenie-dostupa-linux/>