

# **Лабораторная работа № 6**

**Мандатное разграничение прав в Linux**

Абу Сувейлим Мухаммед Мунифович

# Содержание

|          |                                       |           |
|----------|---------------------------------------|-----------|
| <b>1</b> | <b>Цель работы</b>                    | <b>5</b>  |
| <b>2</b> | <b>Задание</b>                        | <b>6</b>  |
| <b>3</b> | <b>Выполнение лабораторной работы</b> | <b>7</b>  |
| <b>4</b> | <b>Выводы</b>                         | <b>16</b> |
|          | <b>Список литературы</b>              | <b>17</b> |

## Список иллюстраций

|      |                                                              |    |
|------|--------------------------------------------------------------|----|
| 3.1  | Коианда <code>getenforce</code> . . . . .                    | 7  |
| 3.2  | Коианда <code>service httpd status</code> . . . . .          | 8  |
| 3.3  | Коианда <code>ps -eZ   grep httpd</code> . . . . .           | 8  |
| 3.4  | Коианда <code>sestatus -b   grep httpd</code> . . . . .      | 9  |
| 3.5  | Коианда <code>seinfo</code> . . . . .                        | 10 |
| 3.6  | Коианда <code>ls -lZ /var/www</code> . . . . .               | 10 |
| 3.7  | html-файл <code>test.html</code> . . . . .                   | 11 |
| 3.8  | html-файл <code>test.html 2</code> . . . . .                 | 11 |
| 3.9  | Коианда <code>man httpd</code> . . . . .                     | 12 |
| 3.10 | Коианда <code>chcon</code> . . . . .                         | 12 |
| 3.11 | Ошибка <code>Forbidden</code> . . . . .                      | 13 |
| 3.12 | Команда <code>ls -l /var/www/html/test.html</code> . . . . . | 13 |
| 3.13 | Лог-файлы . . . . .                                          | 14 |
| 3.14 | Команда <code>semanage</code> . . . . .                      | 14 |
| 3.15 | Команда <code>rm /var/www/html/test.html</code> . . . . .    | 15 |

## **Список таблиц**

# 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.

## 2 Задание

Для проведения указанной лабораторной работы на одно рабочее место требуется компьютер с установленной операционной системой Linux, поддерживающей технологию SELinux. Предполагается использовать стандартный дистрибутив Linux CentOS с включённой политикой SELinux targeted и режимом enforcing. Для выполнения заданий требуется наличие учётной записи администратора (root) и учётной записи обычного пользователя. Постоянно работать от учётной записи root неправильно с точки зрения безопасности [1]

### 3 Выполнение лабораторной работы

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).

```
[smabu@smabu ~]$ getenforce
Enforcing
[smabu@smabu ~]$ 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
[smabu@smabu ~]$
```

Рис. 3.1: Команда `getenforce`

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`. (рис. 3.2):

```

[smabu@smabu ~]$ 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 Sat 2024-10-12 14:07:48 MSK; 1min 3s ago
     Docs: man:httpd.service(8)
   Main PID: 47128 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0 B/sec"
    Tasks: 177 (limit: 47881)
   Memory: 21.8M
      CPU: 67ms
   CGroup: /system.slice/httpd.service
           └─47128 /usr/sbin/httpd -DFOREGROUND
             └─47129 /usr/sbin/httpd -DFOREGROUND
               └─47134 /usr/sbin/httpd -DFOREGROUND
                 └─47135 /usr/sbin/httpd -DFOREGROUND
                   └─47136 /usr/sbin/httpd -DFOREGROUND
[smabu@smabu ~]$

```

Рис. 3.2: Кoiанда service httpd status

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` или `ps -eZ | grep httpd` (рис. 3.3):

```

[root@smabu httpd]# ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 47128 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 47129 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 47134 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 47135 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 47136 ? 00:00:00 httpd
[root@smabu httpd]#

```

Рис. 3.3: Кoiанда ps -eZ | grep httpd

Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды (рис. 3.4):



```

root@smabu httpd]# sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
httpd_can_connect_ldap off
httpd_can_connect_mythtv off
httpd_can_connect_zabbix off
httpd_can_manage_courier_spool off
httpd_can_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
httpd_graceful_shutdown off
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssi_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_comm off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_verify_dns off
root@smabu httpd]#

```

Рис. 3.4: Конец команды `sestatus -b | grep httpd`

Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов (рис. 3.5):

```
[root@smabu httpd]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:      135      Permissions:      457
Sensitivities: 1      Categories:      1024
Types:        5169     Attributes:       259
Users:        8        Roles:           15
Booleans:     358      Cond. Expr.:     390
Allow:        65633    Neverallow:      0
Auditallow:   176      Dontaudit:       8703
Type_trans:   271851   Type_change:     94
Type_member:  37        Range_trans:     5931
Role allow:   40        Role_trans:      417
Constraints:  70        Validatetrans:   0
MLS Constrain: 72      MLS Val. Tran:   0
Permissives:  2        Polcap:          6
Defaults:     7        Typebounds:      0
Allowxperm:   0        Neverallowxperm: 0
Auditallowxperm: 0      Dontauditxperm:  0
Ibendportcon: 0        Ibpkeycon:       0
Initial SIDs: 27        Fs_use:          35
Genfscon:     109      Portcon:         665
Netifcon:     0        Nodecon:         0

[root@smabu httpd]#
```

Рис. 3.5: Коианда seinfo

Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www` (рис. 3.6):

```
[root@smabu httpd]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 авг 12 16:20 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 авг 12 16:20 html
[root@smabu httpd]# ls -lZ /var/www/html
итого 0
[root@smabu httpd]#
```

Рис. 3.6: Коианда ls -lZ /var/www

ОСоздайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания (рис. 3.7):

```
GNU nano 5.6.1
<html>
<body>test</body>
</html>
```

Рис. 3.7: html-файл test.html

Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён (рис. 3.8):

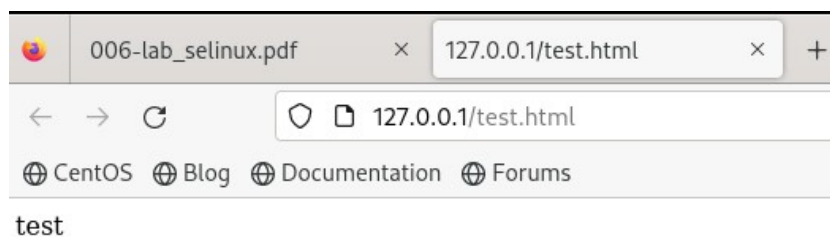


Рис. 3.8: html-файл test.html 2

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. ls -Z /var/www/html/test.htm` (рис. 3.9):

```
HTTPD(8)                                httpd                                HTTPD(8)

NAME
    httpd - Apache Hypertext Transfer Protocol Server

SYNOPSIS
    httpd [ -d serverroot ] [ -f config ] [ -C directive ] [ -c directive ] [ -D parameter ] [ -e level ] [ -E file ] [ -k start|restart|graceful|stop|graceful-stop ] [ -h ] [ -l ] [ -L ] [ -S ] [ -t ] [ -v ] [ -V ] [ -X ] [ -M ] [ -T ]

    On Windows systems, the following additional arguments are available:

    httpd [ -k install|config|uninstall ] [ -n name ] [ -w ]

SUMMARY
    httpd is the Apache HyperText Transfer Protocol (HTTP) server program. It is designed to be run as a stand-alone daemon process. When used like this it will create a pool of child processes or threads to handle requests.

    In general, httpd should not be invoked directly, but rather should be invoked via apachectl on Unix-based systems or as a service on Windows NT, 2000 and XP and as a console application on Windows 9x and ME.

OPTIONS
    -d serverroot
        Set the initial value for the ServerRoot directive to serverroot. This can be overridden by the ServerRoot directive in the configuration file. The default is /etc/httpd.

    -f config
        Uses the directives in the file config on startup. If config does not begin with a /, then it is taken to be a path relative to the ServerRoot. The default is conf/httpd.conf.

    -k start|restart|graceful|stop|graceful-stop
        Signals httpd to start, restart, or stop. See Stopping Apache httpd for more information.

    -C directive
        Process the configuration directive before reading config files.

    -c directive
        Process the configuration directive after reading config files.

    -D parameter
        Sets a configuration parameter which can be used with <IfDefine> sections in the configuration files to conditionally skip or process commands at server startup and restart. Also can be used to set certain less-common startup parameters including -DNO_DETACH (prevent the parent from forking) and -DFOREGROUND (prevent the parent from calling setsid() et al).

    -e level
        Sets the LogLevel to level during server startup. This is useful for temporarily increasing the verbosity of the error messages to find problems during startup.

    -E file
        Send error messages during server startup to file.

    -h
        Output a short summary of available command line options.

    -l
        Output a list of modules compiled into the server. This will not list dynamically loaded modules included using the LoadModule directive.

Manual page httpd(8) line 1 (press h for help or q to quit)
```

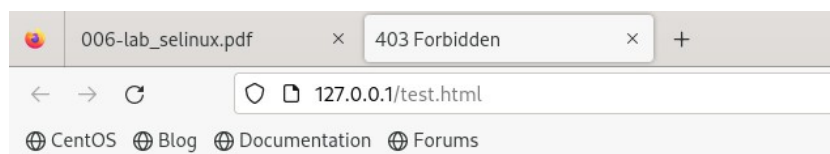
Рис. 3.9: Коианда man httpd

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. 3.10):

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

Рис. 3.10: Коианда chcon

После этого проверьте, что контекст поменялся. 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. 3.11):



## Forbidden

You don't have permission to access this resource.

Рис. 3.11: Ошибка Forbidden

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 `auditd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно (рис. 3.12):

```
[root@smabu httpd]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 32 окт 12 14:21 /var/www/html/test.html
[root@smabu httpd]# tail /var/log/messages
Oct 12 14:27:08 smabu systemd[1]: Started setroubleshoot daemon for processing new SELinux denial logs.
Oct 12 14:27:08 smabu setroubleshoot[48121]: failed to retrieve rpm info for path '/var/www/html/test.html':
Oct 12 14:27:08 smabu systemd[1]: Created slice Slice /system/dbus-1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct 12 14:27:08 smabu systemd[1]: Started dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Oct 12 14:27:09 smabu setroubleshoot[48121]: SELinux запрещает /usr/sbin/httpd доступ getattr к файлу /var/www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l 15df8d74-2488-42a0-99af-89ad74b74564
Oct 12 14:27:09 smabu setroubleshoot[48121]: SELinux запрещает /usr/sbin/httpd доступ getattr к файлу /var/www/html/test.html.#012#012***** Модуль restorecon предлагает (точность 92.2) *****#012#012Если вы хотите исправить метку .STARGET3знак _PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для доступа к родительскому 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 не лечить test.html как общедоступный контент#012То необходимо изменить метку test.html с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v /var/www/html/test.html#012#012***** Модуль catchall предлагает (точность 1.41) *****#012#012Если вы считаете, что httpd должно быть разрешено getattr 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
Oct 12 14:27:09 smabu setroubleshoot[48121]: SELinux запрещает /usr/sbin/httpd доступ getattr к файлу /var/www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l 15df8d74-2488-42a0-99af-89ad74b74564
Oct 12 14:27:09 smabu setroubleshoot[48121]: SELinux запрещает /usr/sbin/httpd доступ getattr к файлу /var/www/html/test.html.#012#012***** Модуль restorecon предлагает (точность 92.2) *****#012#012Если вы хотите исправить метку .STARGET3знак _PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для доступа к родительскому 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 не лечить test.html как общедоступный контент#012То необходимо изменить метку test.html с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v /var/www/html/test.html#012#012***** Модуль catchall предлагает (точность 1.41) *****#012#012Если вы считаете, что httpd должно быть разрешено getattr 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
Oct 12 14:27:19 smabu systemd[1]: dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.
Oct 12 14:27:19 smabu systemd[1]: setroubleshootd.service: Deactivated successfully.
[root@smabu httpd]#
```

Рис. 3.12: Команда `ls -l /var/www/html/test.html`

Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в `/etc/services`). Для этого в фай-

ле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81. 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 (рис. 3.13):

```

root@smabu httpd]# nano /etc/httpd/httpd.conf
root@smabu httpd]# tail /var/log/messages
ct 12 14:27:08 smabu systemd[1]: Started Setroubleshoot daemon for processing new SELinux denial logs.
ct 12 14:27:08 smabu setroubleshoot[4812]: failed to retrieve rpm info for path '/var/www/html/test.html':
ct 12 14:27:08 smabu systemd[1]: Created slice Slice /system/dbus-1.1-org.fedoraproject.SetroubleshootPrivileged.
ct 12 14:27:08 smabu systemd[1]: Started dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
ct 12 14:27:09 smabu setroubleshoot[4812]: SELinux запрещает /usr/sbin/httpd доступ getattr к файлу /var/www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l 15df8d74-2488-42a0-99af-89ad74b74564
ct 12 14:27:09 smabu setroubleshoot[4812]: SELinux запрещает /usr/sbin/httpd доступ getattr к файлу /var/www/html/test.html.#012#012***** Модуль restorecon предлагает (точность 92.2) *****#012#012Если вы хотите исправить метку.$TARGETзнак_PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для доступа к родительскому каталогу, и в этом случае попытайтесь соответствующим образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Модуль public_content предлагает (точность 7.83) *****#012#012Если вы хотите лечить test.html как общедоступный контент#012То необходимо изменить метку test.html с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Модуль catchall предлагает (точность 1.41) *****#012#012Если вы считаете, что httpd должно быть разрешено getattr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012Сделать#012# разрешить этот доступ сейчас, выполнив:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
ct 12 14:27:09 smabu setroubleshoot[4812]: SELinux запрещает /usr/sbin/httpd доступ getattr к файлу /var/www/html/test.html. Для выполнения всех сообщений SELinux: sealert -l 15df8d74-2488-42a0-99af-89ad74b74564
ct 12 14:27:09 smabu setroubleshoot[4812]: SELinux запрещает /usr/sbin/httpd доступ getattr к файлу /var/www/html/test.html.#012#012***** Модуль restorecon предлагает (точность 92.2) *****#012#012Если вы хотите исправить метку.$TARGETзнак_PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для доступа к родительскому 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 изменить метку test.html с public_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Модуль catchall предлагает (точность 1.41) *****#012#012Если вы считаете, что httpd должно быть разрешено getattr доступ к test.html file по умолчанию.#012То рекомендуется создать отчет об ошибке.#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012Сделать#012# разрешить этот доступ сейчас, выполнив:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
ct 12 14:27:19 smabu systemd[1]: dbus-1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.
ct 12 14:27:19 smabu systemd[1]: setroubleshoot.service: Deactivated successfully.
root@smabu httpd]#

```

Рис. 3.13: Лог-файлы

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. 3.14):

```

root@smabu httpd]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
               {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,permissive,dontaudit}
               ...
semanage: error: unrecognized arguments: -p 81
root@smabu httpd]#

```

Рис. 3.14: Команда semanage

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. Исправьте обратно конфигурационный файл apache, вернув Listen 80. Удалите привязку http\_port\_t к 81 порту: semanage port -d -t http\_port\_t -p tcp 81 и

проверьте, что порт 81 удалён. Удалите файл /var/www/html/test.html: rm /var/www/html/test.html (рис. 3.15):

```
[root@smabu httpd]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@smabu httpd]#
```

Рис. 3.15: Команда rm /var/www/html/test.html

## 4 Выводы

Развивли свои навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверили работу SELinx на практике совместно с веб-сервером Apache.



## **Список литературы**

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.