

Отчет по лабораторной работе №6

по дисциплине: Информационная безопасность

Логинов Егор Игоревич

Содержание

1	Цели работы	4
2	Задание	5
3	Теоретическое введение	6
4	Выполнение лабораторной работы	7
5	Выводы	17
6	Список литературы	18

Список иллюстраций

4.1	Конфигурация SELinux	7
4.2	Обращение к веб-серверу	8
4.3	Контекст безопасности веб-сервера Apache	8
4.4	Текущее состояние переключателей SELinux для Apache	9
4.5	Статистика по политике	10
4.6	Тип файлов и поддиректорий, находящихся в директории /var/www	10
4.7	Создание файла /var/www/html/test.html	11
4.8	Файл test.html в браузере	11
4.9	Вызов справки	12
4.10	Изменение контекста	12
4.11	Файл test.html в браузере после изменения контекста	13
4.12	Содержимое логов	13
4.13	Изменение содержимого файла /etc/httpd/httpd.conf	14
4.14	Лог-файл tail -nl /var/log/messages	14
4.15	Попытка добавления порта 81 в список и вывод списка допустимых портов	15
4.16	Повторный запуск веб-сервера	15
4.17	Попытка удаления привязки к порту 81	16

1 Цели работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹. Проверить работу SELinx на практике совместно с веб-сервером Apache.

2 Задание

1. Настроить и запустить сервер Apache.
2. Исследовать влияние параметров сервера на его работу.

3 Теоретическое введение

- Операционная система — это комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем [1].
- Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы. [2].

4 Выполнение лабораторной работы

1. Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted (4.1).

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

Рис. 4.1: Конфигурация SELinux

2. Обратимся с помощью браузера к веб-серверу, запущенному на нашем компьютере, и убедимся, что последний работает (4.2).

```

[yegor@yegor ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[yegor@yegor ~]$ 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 2023-10-14 15:07:28 MSK; 5s ago
     Docs: man:httpd.service(8)
  Main PID: 41219 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 12196)
    Memory: 32.3M
       CPU: 147ms
    CGroup: /system.slice/httpd.service
            └─41219 /usr/sbin/httpd -DFOREGROUND
              └─41228 /usr/sbin/httpd -DFOREGROUND
                └─41229 /usr/sbin/httpd -DFOREGROUND
                  └─41230 /usr/sbin/httpd -DFOREGROUND
                    └─41231 /usr/sbin/httpd -DFOREGROUND

окт 14 15:07:22 yegor.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 14 15:07:28 yegor.localdomain httpd[41219]: Server configured, listening on: port 80
окт 14 15:07:28 yegor.localdomain systemd[1]: Started The Apache HTTP Server.
[yegor@yegor ~]$

```

Рис. 4.2: Обращение к веб-серверу

3. Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности (4.3).

```

[yegor@yegor ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      41219  0.1  0.5 20328 11508 ?        Ss   15:07   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  41228  0.0  0.3 21664 7296 ?        S    15:07   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  41229  0.0  0.7 2521332 15012 ?      Sl   15:07   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  41230  0.0  0.5 2324660 10920 ?      Sl   15:07   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  41231  0.0  0.6 2324660 12968 ?      Sl   15:07   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0.c1023 yegor  41490  0.0  0.1 221688 2304 pts/0  S+   15:08   0:00 grep --color=auto h
[yegor@yegor ~]$

```

Рис. 4.3: Контекст безопасности веб-сервера Apache

4. Посмотрим текущее состояние переключателей SELinux для Apache (4.4).


```
[yegor@yegor ~]$ 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
```

Рис. 4.4: Текущее состояние переключателей SELinux для Apache

5. Посмотрим статистику по политике с помощью команды `seinfo` (4.5).

```

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:            5100     Attributes:           258
Users:            8        Roles:                14
Booleans:         353     Cond. Expr.:         384
Allow:            65000    Neverallow:           0
Auditallow:       170     Dontaudit:           8572
Type_trans:       265341   Type_change:          87
Type_member:      35      Range_trans:         6164
Role allow:       38      Role_trans:          420
Constraints:      70     Validatetrans:        0
MLS Constrains:  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:              660
Netifcon:        0      Nodecon:              0

```

Рис. 4.5: Статистика по политике

6. Определим тип файлов и поддиректорий, находящихся в директориях /var/www и /var/www/html. Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html(4.6).

```

[yegor@yegor ~]$ ls -lZ /var/www/
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 мая 16 23:21 html
[yegor@yegor ~]$ ls -lZ /var/www/html/
итого 0
[yegor@yegor ~]$ █

```

Рис. 4.6: Тип файлов и поддиректорий, находящихся в директории /var/www

7. Создадим от имени суперпользователя html-файл /var/www/html/test.html.
Проверим контекст созданного нами файла (4.7).

```
[yegor@yegor ~]$ sudo su
[root@yegor yegor]# nano /var/www/html/test.html
[root@yegor yegor]# ls -lZ /var/www/html/
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 окт 14 15:13 test.ht
[root@yegor yegor]#
```

Рис. 4.7: Создание файла /var/www/html/test.html

Заполним его следующим содержимым:

```
<html>
  <body>test</body>
</html>
```

Как видим по умолчанию присваивается контекст *unconfined_u:object_r:httpd_sys_content_t:s0*

8. Обратимся к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>.
Убедимся, что файл был успешно отображён (4.8).

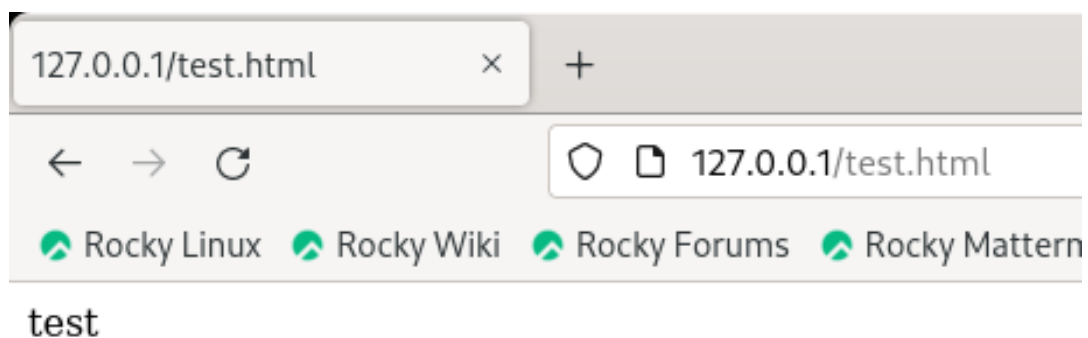
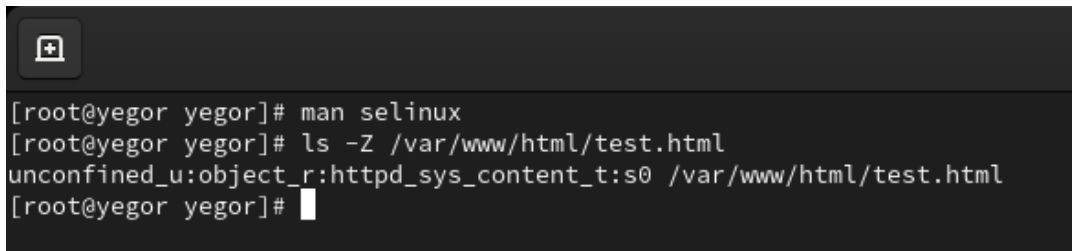


Рис. 4.8: Файл test.html в браузере

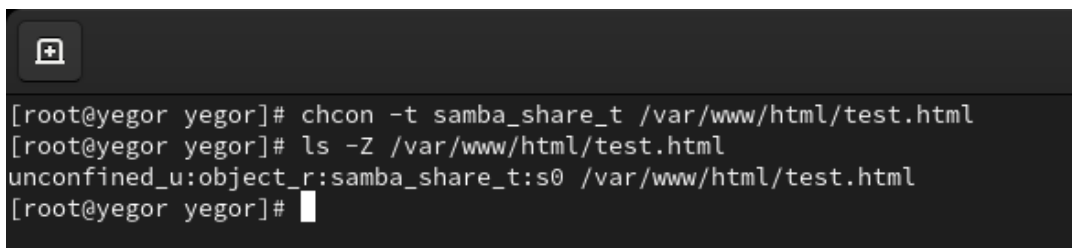
9. Изучим справку `man httpd_selinux` и выясним, какие контексты файлов определены для `httpd`. Сопоставим их с типом файла `test.html` (4.9).

A terminal window with a dark background and a terminal icon in the top-left corner. The terminal shows the following commands and output:

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

Рис. 4.9: Вызов справки

10. Изменим контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t` (4.10).

A terminal window with a dark background and a terminal icon in the top-left corner. The terminal shows the following commands and output:

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

Рис. 4.10: Изменение контекста

11. Попробуем ещё раз получить доступ к файлу через веб-сервер (4.11).

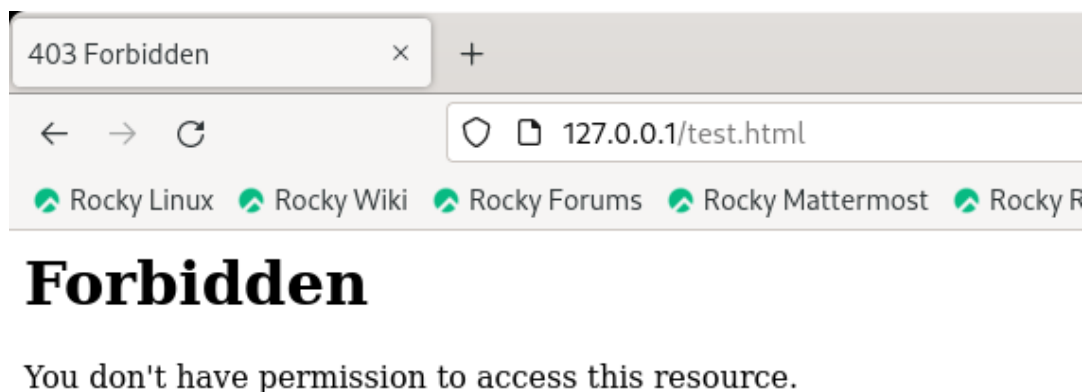


Рис. 4.11: Файл test.html в браузере после изменения контекста

12. Просмотрим log-файлы веб-сервера Apache и системный лог-файл (4.12).

```

[root@yegor yegor]# chcon -t samba_share_t /var/www/html/test.html
[root@yegor yegor]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@yegor yegor]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 окт 14 15:13 /var/www/html/test.html
[root@yegor yegor]# tail /var/log/messages
Oct 14 15:19:19 yegor systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged.
Oct 14 15:19:19 yegor systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Oct 14 15:19:21 yegor setroubleshoot[42209]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/
авить метку.$TARGETЗнак _PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете запустить restorecon. Во
ае попытаться соответствующим образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /var/www/html/
ить test.html как общедоступный контент#012То необходимо изменить метку test.html с public_content_t на public_cont
tml/test.html'#012#012***** Модуль catchall предлагает (точность 1.41) *****#012#012Если вы
об ошибке.#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ
Oct 14 15:19:21 yegor setroubleshoot[42209]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/
Oct 14 15:19:21 yegor setroubleshoot[42209]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/
авить метку.$TARGETЗнак _PATH по умолчанию должен быть httpd_sys_content_t#012То вы можете запустить restorecon. Во
ае попытаться соответствующим образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /var/www/html/
ить test.html как общедоступный контент#012То необходимо изменить метку test.html с public_content_t на public_cont
tml/test.html'#012#012***** Модуль catchall предлагает (точность 1.41) *****#012#012Если вы
об ошибке.#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ
Oct 14 15:19:31 yegor systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated succe
Oct 14 15:19:31 yegor systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 1.620s C
Oct 14 15:19:31 yegor systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct 14 15:19:31 yegor systemd[1]: setroubleshootd.service: Consumed 1.272s CPU time.
[root@yegor yegor]#

```

Рис. 4.12: Содержимое логов

Как видим, нам не удалось получить доступ к файлу как раз из-за измененного контекста.

13. Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81. Выполним перезапуск веб-сервера. Сбоя не произошло (4.13).

```
[root@yegor yegor]# nano /etc/httpd/conf/httpd.conf
[root@yegor yegor]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@yegor yegor]# 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 2023-10-14 15:23:15 MSK; 5s ago
     Docs: man:httpd.service(8)
  Main PID: 42316 (httpd)
    Status: "Started, listening on: port 81"
     Tasks: 213 (limit: 12196)
    Memory: 41.6M
       CPU: 140ms
    CGroup: /system.slice/httpd.service
            └─42316 /usr/sbin/httpd -DFOREGROUND
              └─42317 /usr/sbin/httpd -DFOREGROUND
                └─42318 /usr/sbin/httpd -DFOREGROUND
                  └─42319 /usr/sbin/httpd -DFOREGROUND
                    └─42323 /usr/sbin/httpd -DFOREGROUND

окт 14 15:23:14 yegor.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 14 15:23:15 yegor.localdomain httpd[42316]: Server configured, listening on: port 81
окт 14 15:23:15 yegor.localdomain systemd[1]: Started The Apache HTTP Server.
[root@yegor yegor]#
```

Рис. 4.13: Изменение содержимого файла /etc/httpd/httpd.conf

14. Проанализируем лог-файлы (4.14).

```
[root@yegor yegor]# tail -nl /var/log/messages
tail: неверное количество строк: «l»
[root@yegor yegor]# tail /var/log/messages
Oct 14 15:19:31 yegor systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivilege
Oct 14 15:19:31 yegor systemd[1]: setroubleshootd.service: Deactivated successfully.
Oct 14 15:19:31 yegor systemd[1]: setroubleshootd.service: Consumed 1.272s CPU time.
Oct 14 15:23:13 yegor systemd[1]: Stopping The Apache HTTP Server...
Oct 14 15:23:14 yegor systemd[1]: httpd.service: Deactivated successfully.
Oct 14 15:23:14 yegor systemd[1]: Stopped The Apache HTTP Server.
Oct 14 15:23:14 yegor systemd[1]: httpd.service: Consumed 1.813s CPU time.
Oct 14 15:23:14 yegor systemd[1]: Starting The Apache HTTP Server...
Oct 14 15:23:15 yegor httpd[42316]: Server configured, listening on: port 81
Oct 14 15:23:15 yegor systemd[1]: Started The Apache HTTP Server.
```

Рис. 4.14: Лог-файл tail -nl /var/log/messages

15. Выполним команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверим список портов командой `semanage port -l | grep http_port_t` Убедимся, что порт 81 есть в списке. (4.15).

```
[root@yegor yegor]# semanage port -m -t http_port_t -p tcp 81
usage: semanage [-h] {import,export,login,user,port,ibpkey,ibendport,interface,module,r
semanage: error: unrecognized arguments: -p 81
[root@yegor yegor]# semanage port -a -t http_port_t --proto tcp 81
ValueError: Порт tcp/81 уже определен
[root@yegor yegor]# semanage port -m -t http_port_t --proto tcp 81
[root@yegor yegor]# semanage prot -l | grep http_port_t
semanage: error: argument subcommand: invalid choice: 'prot' (choose from 'import', 'ex
[root@yegor yegor]# semanage port -l | grep http_port_t
http_port_t          tcp      81, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@yegor yegor]#
```

Рис. 4.15: Попытка добавления порта 81 в список и вывод списка допустимых портов

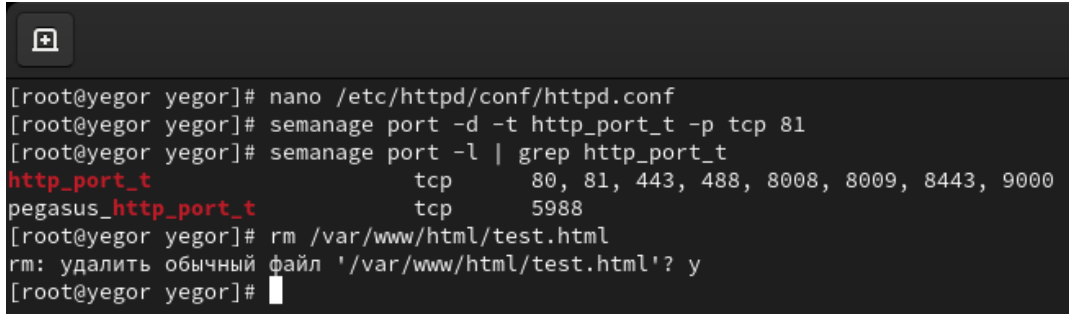
16. Попробуем запустить веб-сервер Apache ещё раз. Вернем контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`. Попробуем получить доступ к файлу через веб-сервер (4.16).

```
[root@yegor yegor]# service httpd stop
Redirecting to /bin/systemctl stop httpd.service
[root@yegor yegor]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@yegor yegor]# 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 2023-10-14 15:33:03 MSK; 4s ago
     Docs: man:httpd.service(8)
  Main PID: 42710 (httpd)
    Status: "Started, listening on: port 81"
   Tasks: 213 (limit: 12196)
  Memory: 35.6M
     CPU: 108ms
  CGroup: /system.slice/httpd.service
          └─42710 /usr/sbin/httpd -DFOREGROUND
            └─42711 /usr/sbin/httpd -DFOREGROUND
              └─42712 /usr/sbin/httpd -DFOREGROUND
                └─42713 /usr/sbin/httpd -DFOREGROUND
                  └─42714 /usr/sbin/httpd -DFOREGROUND

окт 14 15:33:03 yegor.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 14 15:33:03 yegor.localdomain httpd[42710]: Server configured, listening on: port 81
окт 14 15:33:03 yegor.localdomain systemd[1]: Started The Apache HTTP Server.
[root@yegor yegor]#
```

Рис. 4.16: Повторный запуск веб-сервера

17. Исправим обратно конфигурационный файл apache, вернув Listen 80. Попробуем удалить привязку http_port_t к 81. Удалим файл /var/www/html/test.html (4.17).



```
[root@yegor yegor]# nano /etc/httpd/conf/httpd.conf
[root@yegor yegor]# semanage port -d -t http_port_t -p tcp 81
[root@yegor yegor]# 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@yegor yegor]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@yegor yegor]#
```

Рис. 4.17: Попытка удаления привязки к порту 81

5 Выводы

В рамках данной лабораторной работы были развиты навыки администрирования ОС Linux. Получено первое практическое знакомство с технологией SELinux¹. Проверена работа SELinux на практике совместно с веб-сервером Apache.

6 Список литературы

1. Операционные системы [Электронный ресурс]. URL: <https://softline.tm/solutions/programmnoe-obespechenie/operating-system>.
2. Права доступа [Электронный ресурс]. URL: <https://w.wiki/7UBB>.