Российский университет дружбы народов

Факультет физико-математических и естественных наук

ОТЧЕТ по лабораторной работе №6

дисциплина: Информационная безопасность

Студент: Васильева Юлия

Группа: НФИбд-03-18

МОСКВА 2021г.

Цель работы

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

Выполнение лабораторной работы

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

```
[yivasileva@yivasileva conf]$ getenforce
Enforcing
[yivasileva@yivasileva 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
Max kernel policy version:      31
[yivasileva@yivasileva conf]$ 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 prese
t: disabled)
   Active: active (running) since Сб 2021-11-2[ 12:27:29 MSK; 54min ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 3693 (httpd)
   Status: "Total requests: 10; Current requests/sec: 0; Current traffic:   0 B/
sec"
    Tasks: 9
   CGroup: /system.slice/httpd.service
           ├─3693 /usr/sbin/httpd -DFOREGROUND
           ├─3698 /usr/sbin/httpd -DFOREGROUND
           ├─3699 /usr/sbin/httpd -DFOREGROUND
           ├─3700 /usr/sbin/httpd -DFOREGROUND
           ├─3701 /usr/sbin/httpd -DFOREGROUND
           ├─3702 /usr/sbin/httpd -DFOREGROUND
```

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 или ps -eZ | grep httpd

```
[yivasileva@yivasileva conf]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root      3693  0.0  0.0 230440   396 ?        Ss   12:27   0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3698  0.0  0.0 232660    44 ?        S    12:27   0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3699  0.0  0.0 232524   100 ?        S    12:27   0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3700  0.0  0.0 232524    28 ?        S    12:27   0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3701  0.0  0.0 232524    28 ?        S    12:27   0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3702  0.0  0.0 232660    72 ?        S    12:27   0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3853  0.0  0.0 232524    28 ?        S    12:31   0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3854  0.0  0.0 232524    28 ?        S    12:31   0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3855  0.0  0.0 232524    28 ?        S    12:31   0:0
0 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 yivasil+ 5651 0.0  0.0 112832 972 pts/0 R
+ 13:22   0:00 grep --color=auto 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».

```
[yivasileva@yivasileva conf]$ 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
Max kernel policy version:      31

Policy booleans:
abrt_anon_write                             off
abrt_handle_event                           off
abrt_upload_watch_anon_write                on
antivirus_can_scan_system                   off
antivirus_use_jit                           off
auditadm_exec_content                       on
authlogin_nsswitch_use_ldap                 off
authlogin_radius                            off
authlogin_yubikey                           off
awstats_purge_apache_log_files              off
boinc_execmem                               on
cdrecord_read_content                       off
cluster_can_network_connect                 off
cluster_manage_all_files                    off
cluster_use_execmem                         off
cobbler_anon_write                          off
cobbler_can_network_connect                 off
cobbler_use_cifs                            off
cobbler_use_nfs                             off
collectd_tcp_network_connect                off
condor_tcp_network_connect                  off
```

5. Посмотрите статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов.
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
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: test
10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html.

```
[yivasileva@yivasileva conf]$ seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

   Classes:            130    Permissions:       272
   Sensitivities:        1    Categories:       1024
   Types:             4793    Attributes:        253
   Users:                8    Roles:              14
   Booleans:           316    Cond. Expr.:       362
   Allow:           107834    Neverallow:          0
   Auditallow:         158    Dontaudit:       10022
   Type_trans:       18153    Type_change:        74
   Type_member:         35    Role allow:         37
   Role_trans:         414    Range_trans:      5899
   Constraints:        143    Validatetrans:       0
   Initial SIDs:        27    Fs_use:             32
   Genfscon:           103    Portcon:           614
   Netifcon:             0    Nodecon:             0
   Permissives:          0    Polcap:              5

[yivasileva@yivasileva conf]$ ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[yivasileva@yivasileva conf]$ ls -lZ /var/www/html
[yivasileva@yivasileva conf]$ echo "<html>" > /var/www/html/test.html
bash: /var/www/html/test.html: Отказано в доступе
[yivasileva@yivasileva conf]$ su
Пароль:
[root@yivasileva conf]# echo "<html>" > /var/www/html/test.html
[root@yivasileva conf]# nano /var/www/html/test.html
[root@yivasileva conf]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@yivasileva conf]# touch /var/www/html/test2.html
[root@yivasileva conf]# cat /var/www/html/test2.html
[root@yivasileva conf]#
```

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедитесь, что файл был успешно отображён.
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. 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*syscontent*t позволяет процессу httpd получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.
13. Измените контекст файла /var/www/html/test.html с httpd*syscontent*t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba*sharet: chcon -t samba*share_t /var/www/html/test.html ls -Z /var/www/html/test.html Информационная безопасность компьютерных сетей 43 После этого проверьте, что контекст поменялся.
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.
15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? ls -l /var/www/html/test.html

```
[yivasileva@yivasileva conf]$ ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[yivasileva@yivasileva conf]$ chcon -t samba_share_t /var/www/html/test.html
chcon: не удалось изменить контекст безопасности «/var/www/html/test.html» на «unconfined_u:obj
ect_r:samba_share_t:s0»: Операция не позволена
[yivasileva@yivasileva conf]$ su
Пароль:
[root@yivasileva conf]# chcon -t samba_share_t /var/www/html/test.html
[root@yivasileva conf]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@yivasileva conf]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 ноя 27 13:39 /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.

```
[root@yivasileva conf]# tail /var/log/messages
Nov 27 13:50:39 yivasileva dbus[726]: [system] Activating service name='org.fedoraproject.Setro
ubleshootd' (using servicehelper)
Nov 27 13:50:41 yivasileva dbus[726]: [system] Successfully activated service 'org.fedoraprojec
t.Setroubleshootd'
Nov 27 13:50:41 yivasileva setroubleshoot: failed to retrieve rpm info for /var/www/html/test.h
tml
Nov 27 13:50:42 yivasileva setroubleshoot: SELinux is preventing httpd from getattr access on t
he file /var/www/html/test.html. For complete SELinux messages run: sealert -l 88b41eaf-6908-4a
bc-931b-ff4368e47a7a
Nov 27 13:50:42 yivasileva python: SELinux is preventing httpd from getattr access 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
 stopped due to insufficient permissions to access a parent directory in which case try to chan
ge the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#01
2#012*****  Plugin public_content (7.83 confidence) suggests   ********************#012#012If y
ou want to treat test.html as public content#012Then you need to change the label on test.html
to public_content_t or public_content_rw_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 ca
tchall (1.41 confidence) suggests   ************************#012#012If you believe that httpd
 should be allowed getattr access on the test.html file by default.#012Then you should report t
```

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.
17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? Сбоя не произошло так как порт 81 изначально указан в установленной политике.

```
r/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=CRED_DISP msg=audit(1638010201.332:474): pid=6376 uid=0 auid=0 ses=12 subj=system_u:system
_r:crond_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/us
r/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=USER_END msg=audit(1638010201.338:475): pid=6376 uid=0 auid=0 ses=12 subj=system_u:system_
r:crond_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_loginuid,pam_keyinit,pam_limits
,pam_systemd acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'
type=SERVICE_STOP msg=audit(1638010215.879:476): pid=1 uid=0 auid=4294967295 ses=4294967295 sub
j=system_u:system_r:init_t:s0 msg='unit=fprintd comm="systemd" exe="/usr/lib/systemd/systemd" h
ostname=? addr=? terminal=? res=success'
type=AVC msg=audit(1638010236.688:477): avc:  denied  { getattr } for  pid=3853 comm="httpd" pa
th="/var/www/html/test.html" dev="dm-0" ino=18431611 scontext=system_u:system_r:httpd_t:s0 tcon
text=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1638010236.688:477): arch=c000003e syscall=4 success=no exit=-13 a0=558c
429aab60 a1=7ffc607683e0 a2=7ffc607683e0 a3=7fc364682772 items=0 ppid=3693 pid=3853 auid=429496
7295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295
comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)
type=PROCTITLE msg=audit(1638010236.688:477): proctitle=2F7573722F7362696E2F687474706400 2D44464
F524547524F554E44
type=AVC msg=audit(1638010236.689:478): avc:  denied  { getattr } for  pid=3853 comm="httpd" pa
th="/var/www/html/test.html" dev="dm-0" ino=18431611 scontext=system_u:system_r:httpd_t:s0 tcon
text=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1638010236.689:478): arch=c000003e syscall=6 success=no exit=-13 a0=558c
429aac40 a1=7ffc607683e0 a2=7ffc607683e0 a3=0 items=0 ppid=3693 pid=3853 auid=4294967295 uid=48
 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd
" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)
type=PROCTITLE msg=audit(1638010236.689:478): proctitle=2F7573722F7362696E2F687474706400 2D44464
F524547524F554E44
[root@yivasileva conf]# nano /var/log/audit/audit.log
[root@yivasileva conf]# nano /etc/httpd/conf/httpd.conf
[root@yivasileva conf]# sudo service apache2 restart
Redirecting to /bin/systemctl restart apache2.service
Failed to restart apache2.service: Unit not found.
[root@yivasileva conf]# sudo service apache restart
Redirecting to /bin/systemctl restart apache.service
Failed to restart apache.service: Unit not found.
[root@yivasileva conf]# sudo systemctl restart httpd.service
[root@yivasileva conf]#
```

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.

```
  GNU nano 2.3.1         Файл: /var/log/httpd/error_log

[Sat Nov 27 12:27:29.447912 2021] [core:notice] [pid 3693] SELinux policy enabl$
[Sat Nov 27 12:27:29.452083 2021] [suexec:notice] [pid 3693] AH01232: suEXEC me$
AH00558: httpd: Could not reliably determine the server's fully qualified domai$
[Sat Nov 27 12:27:29.491162 2021] [lbmethod_heartbeat:notice] [pid 3693] AH0228$
[Sat Nov 27 12:27:29.493781 2021] [mpm_prefork:notice] [pid 3693] AH00163: Apac$
[Sat Nov 27 12:27:29.493817 2021] [core:notice] [pid 3693] AH00094: Command lin$
[Sat Nov 27 12:31:25.882661 2021] [autoindex:error] [pid 3702] [client 10.0.2.1$
[Sat Nov 27 13:50:36.702037 2021] [core:error] [pid 3853] (13)Permission denied$
[Sat Nov 27 14:02:50.752136 2021] [mpm_prefork:notice] [pid 3693] AH00170: caug$
[Sat Nov 27 14:02:51.936790 2021] [core:notice] [pid 6718] SELinux policy enabl$
[Sat Nov 27 14:02:51.940816 2021] [suexec:notice] [pid 6718] AH01232: suEXEC me$
[Sat Nov 27 14:02:51.952261 2021] [lbmethod_heartbeat:notice] [pid 6718] AH0228$
[Sat Nov 27 14:02:51.954235 2021] [mpm_prefork:notice] [pid 6718] AH00163: Apac$
[Sat Nov 27 14:02:51.954267 2021] [core:notice] [pid 6718] AH00094: Command lin$

                [ Прочитано 14 строк ]
^G Помощь     ^O Записать  ^R ЧитФайл  ^Y ПредСтр   ^K Вырезать  ^C ТекПозиц
^X Выход      ^J Выровнять ^W Поиск     ^V СледСтр   ^U ОтмВырезк ^T Словарь
```

```
  GNU nano 2.3.1         Файл: /var/log/httpd/access_log

10.0.2.15 - - [27/Nov/2021:12:31:25 +0300] "GET / HTTP/1.1" 403 4897 "-" "Mozil$
10.0.2.15 - - [27/Nov/2021:12:31:25 +0300] "GET /noindex/css/bootstrap.min.css $
10.0.2.15 - - [27/Nov/2021:12:31:25 +0300] "GET /noindex/css/open-sans.css HTTP$
10.0.2.15 - - [27/Nov/2021:12:31:25 +0300] "GET /images/apache_pb.gif HTTP/1.1"$
10.0.2.15 - - [27/Nov/2021:12:31:25 +0300] "GET /images/poweredby.png HTTP/1.1"$
10.0.2.15 - - [27/Nov/2021:12:31:26 +0300] "GET /favicon.ico HTTP/1.1" 404 209 $
10.0.2.15 - - [27/Nov/2021:12:31:26 +0300] "GET /noindex/css/fonts/Light/OpenSa$
10.0.2.15 - - [27/Nov/2021:12:31:26 +0300] "GET /noindex/css/fonts/Bold/OpenSan$
10.0.2.15 - - [27/Nov/2021:12:31:26 +0300] "GET /noindex/css/fonts/Light/OpenSa$
10.0.2.15 - - [27/Nov/2021:12:31:26 +0300] "GET /noindex/css/fonts/Bold/OpenSan$
127.0.0.1 - - [27/Nov/2021:13:43:00 +0300] "GET /test.html HTTP/1.1" 200 33 "-"$
127.0.0.1 - - [27/Nov/2021:13:43:00 +0300] "GET /favicon.ico HTTP/1.1" 404 209 $
127.0.0.1 - - [27/Nov/2021:13:45:53 +0300] "GET /test.html HTTP/1.1" 200 33 "-"$
127.0.0.1 - - [27/Nov/2021:13:45:53 +0300] "GET /favicon.ico HTTP/1.1" 404 209 $
127.0.0.1 - - [27/Nov/2021:13:50:36 +0300] "GET /test.html HTTP/1.1" 403 211 "-$



                [ Прочитано 15 строк ]
^G Помощь     ^O Записать  ^R ЧитФайл   ^Y ПредСтр   ^K Вырезать  ^C ТекПозиц
^X Выход      ^J Выровнять ^W Поиск     ^V СледСтр   ^U ОтмВырезк ^T Словарь
```

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.
20. Попробуйте запустить веб-сервер Apache ещё раз. Поняли ли вы, почему он сейчас запустился, а в предыдущем случае не смог? В данном случае не запустился бы, по причине отсутствия привязки порта 81 к http*port*t.
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 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».

```
[root@yivasileva yivasileva]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@yivasileva yivasileva]# 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@yivasileva yivasileva]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@yivasileva yivasileva]# 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 prese
t: disabled)
   Active: active (running) since Сб 2021-11-27 14:02:51 MSK; 11min ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 6712 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCC
ESS)
 Main PID: 6718 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/s
ec"
    Tasks: 6
   CGroup: /system.slice/httpd.service
           ├─6718 /usr/sbin/httpd -DFOREGROUND
           ├─6719 /usr/sbin/httpd -DFOREGROUND
           ├─6720 /usr/sbin/httpd -DFOREGROUND
           ├─6721 /usr/sbin/httpd -DFOREGROUND
           ├─6722 /usr/sbin/httpd -DFOREGROUND
           └─6723 /usr/sbin/httpd -DFOREGROUND

ноя 27 14:02:51 yivasileva.localdomain systemd[1]: Starting The Apache HTT...
ноя 27 14:02:51 yivasileva.localdomain systemd[1]: Started The Apache HTTP...
Hint: Some lines were ellipsized, use -l to show in full.
[root@yivasileva yivasileva]# chcon -t httpd_sys_content_t /var/www/html/test.ht
ml
```

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

```
[root@yivasileva yivasileva]# nano /etc/httpd/conf/httpd.conf
[root@yivasileva yivasileva]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@yivasileva yivasileva]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@yivasileva yivasileva]#
```

Вывод

Мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.