

# **Лабораторная работа №6**

**Мандатное разграничение прав в Linux**

Кувшинова К.О. группа НФИ-02-19

# Содержание

1	Цель работы	4
2	Подготовка лабораторного стенда и методические рекомендации	5
3	Выполнение лабораторной работы	7
4	Вывод	18
5	Библиография	19

# List of Figures

2.1	Установка веб-сервера Apache . . . . .	5
2.2	Установка параметра ServerName . . . . .	5
2.3	Отключение пакетного фильтра . . . . .	6
3.1	Выполнение команд <code>getenforce</code> и <code>sestatus</code> . . . . .	7
3.2	Выполнение команд <code>service httpd start</code> и <code>status</code> . . . . .	8
3.3	Выполнение команды <code>ps auxZ   grep httpd</code> . . . . .	8
3.4	Выполнение команды <code>sestatus -b   grep httpd</code> . . . . .	9
3.5	Статистика по политике . . . . .	10
3.6	Выполнение команды <code>ls -lZ /var/www</code> . . . . .	10
3.7	Выполнение команды <code>ls -lZ /var/www/html</code> . . . . .	11
3.8	Выполнение команды <code>ls -lZ /var/www</code> . . . . .	11
3.9	Содержимое файла <code>test.html</code> . . . . .	11
3.10	Контекст файла <code>test.html</code> . . . . .	12
3.11	Обращение к файлу <code>test.html</code> через веб-сервер . . . . .	12
3.12	Контекст файла <code>test.html</code> . . . . .	12
3.13	Изменение контекста файла <code>/var/www/html/test.html</code> . . . . .	13
3.14	Обращение к файлу <code>test.html</code> через веб-сервер после изменения контекста . . . . .	13
3.15	Вывод команд <code>ls -l /var/www/html/test.html</code> и <code>tail /var/log/messages</code> . . . . .	14
3.16	Запуск веб-сервера Apache на прослушивание TCP-порта 81 . . . . .	14
3.17	Перезапуск веб-сервера Apache . . . . .	15
3.18	Проверка установления 81 порта tcp . . . . .	15
3.19	Перезапуск веб-сервера Apache . . . . .	15
3.20	Возвращение контекста <code>httpd_sys_content_t</code> к файлу <code>test.html</code> . . . . .	15
3.21	Обращение к файлу <code>test.html</code> через веб-сервер . . . . .	16
3.22	Исправление конфигурационного файла <code>apache</code> . . . . .	16
3.23	Удаление привязки <code>http_port_t</code> к 81 порту . . . . .	16
3.24	Удаление файла <code>test.html</code> . . . . .	17

# 1 Цель работы

Целью данной лабораторной работы является развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinx на практике совместно с веб-сервером Apache.

## 2 Подготовка лабораторного стенда и методические рекомендации

1. Установили веб-сервер Apache командой **yum install httpd**. (fig. 2.1)

```
[root@kokuvshinova kokuvshinova]# yum install httpd
Rocky Linux 9 - BaseOS              7.1 kB/s | 3.6 kB      00:00
Rocky Linux 9 - BaseOS              1.7 MB/s | 1.7 MB      00:00
Rocky Linux 9 - AppStream           6.9 kB/s | 3.6 kB      00:00
Rocky Linux 9 - AppStream           3.2 MB/s | 6.0 MB      00:01
Rocky Linux 9 - Extras              5.5 kB/s | 2.9 kB      00:00
Зависимости разрешены.
=====
Пакет                Архитектура Версия                Репозиторий    Размер
=====
Установка:
  httpd                x86_64      2.4.51-7.el9_0          appstream      1.4 М
Установка зависимостей:
```

Figure 2.1: Установка веб-сервера Apache

2. В конфигурационном файле `/etc/httpd/httpd.conf` задали параметр `ServerName`. (fig. 2.2)

```
[root@kokuvshinova kokuvshinova]# cd /etc/httpd
[root@kokuvshinova httpd]# echo "ServerName test.ru" >> httpd.conf
```

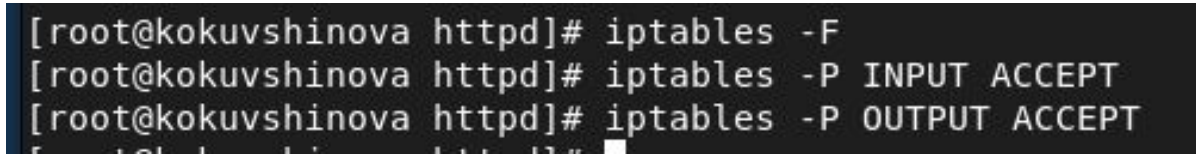
Figure 2.2: Установка параметра `ServerName`

3. Отключаем пакетный фильтр с помощью команд: (fig. 2.3)

`iptables -F`

`iptables -P INPUT ACCEPT`

iptables -P OUTPUT ACCEPT

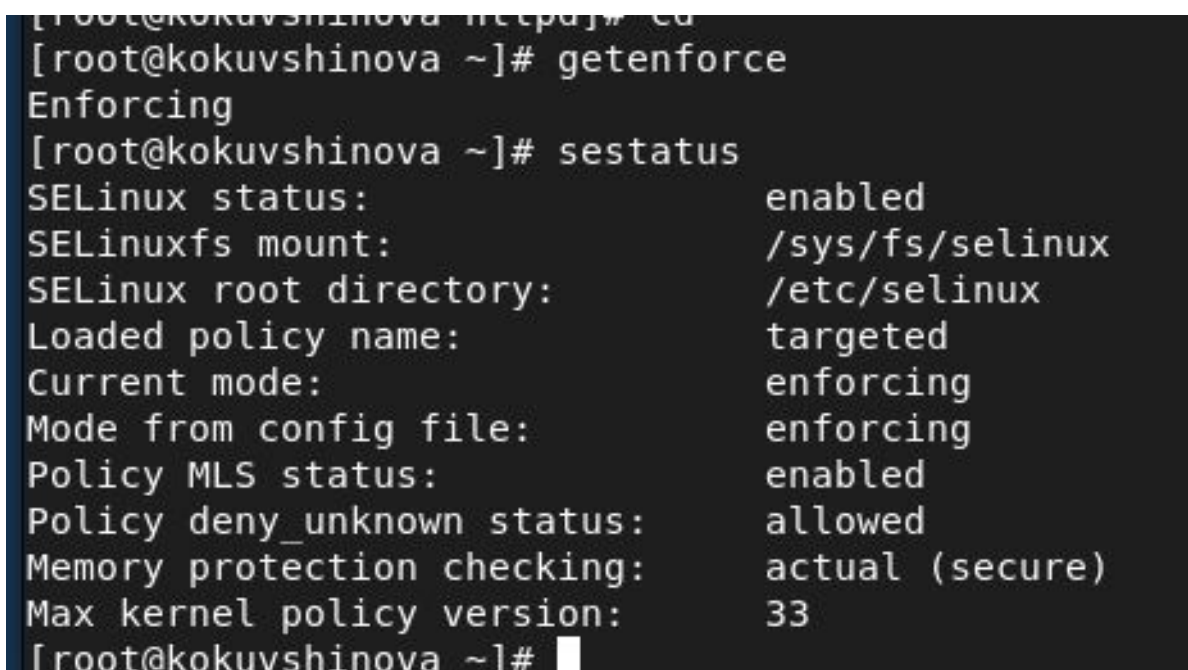
A terminal window with a dark background and light-colored text. It shows three lines of commands being executed as root on a system named kokuvshinova. The first line flushes the iptables ruleset. The second line sets the default policy for the INPUT chain to ACCEPT. The third line sets the default policy for the OUTPUT chain to ACCEPT.

```
[root@kokuvshinova httpd]# iptables -F
[root@kokuvshinova httpd]# iptables -P INPUT ACCEPT
[root@kokuvshinova httpd]# iptables -P OUTPUT ACCEPT
```

Figure 2.3: Отключение пакетного фильтра

### 3 Выполнение лабораторной работы

1. Входим в систему с полученными учётными данными. Проверили, что SELinux работает в режиме enforcing политики targeted с помощью команд **getenforce** и **sestatus**. (fig. 3.1)

A terminal window with a dark background and light-colored text. The prompt is [root@kokuvshinova ~]#. The first command executed is getenforce, which returns Enforcing. The second command is sestatus, which returns a detailed status of SELinux. The output of sestatus is as follows:

```
[root@kokuvshinova ~]# getenforce
Enforcing
[root@kokuvshinova ~]# 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@kokuvshinova ~]#
```

Figure 3.1: Выполнение команд getenforce и sestatus

2. Запустили веб-сервер и обратились к нему с помощью команд (fig. 3.2): `service httpd start` `service httpd status`

```

[root@kokuvshinova etc]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@kokuvshinova etc]# 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 2022-10-10 17:09:27 MSK; 10s ago
     Docs: man:httpd.service(8)
   Main PID: 39619 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/0"
    Tasks: 213 (limit: 12210)
   Memory: 26.2M
      CPU: 95ms
   CGroup: /system.slice/httpd.service
           └─39619 /usr/sbin/httpd -DFOREGROUND
             └─39620 /usr/sbin/httpd -DFOREGROUND
               └─39624 /usr/sbin/httpd -DFOREGROUND
                 └─39625 /usr/sbin/httpd -DFOREGROUND
                   └─39626 /usr/sbin/httpd -DFOREGROUND

окт 10 17:09:27 kokuvshinova.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 10 17:09:27 kokuvshinova.localdomain systemd[1]: Started The Apache HTTP Server.
окт 10 17:09:27 kokuvshinova.localdomain httpd[39619]: Server configured, listening on:
[root@kokuvshinova etc]#

```

Figure 3.2: Выполнение команд `service httpd start` и `status`

3. Найшли веб-сервер Apache в списке процессов с помощью команды **ps auxZ | grep httpd**. Контекст безопасности - `unconfined_u:unconfined_r:unconfined_t`. (fig. 3.3)

```

[root@kokuvshinova ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      39619  0.0  0.5 20248 11704 ?        Ss   17:09
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  39620  0.0  0.3 21572  7444 ?        S    17:09
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  39624  0.0  0.5 1079376 11100 ?        Sl   17:09
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  39625  0.0  0.6 1210512 13148 ?        Sl   17:09
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  39626  0.0  0.5 1079376 11100 ?        Sl   17:09
0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 40041  0.0  0.1 221692 2292 pts/0 S
+ 17:30 0:00 grep --color=auto httpd

```

Figure 3.3: Выполнение команды `ps auxZ | grep httpd`

4. Посмотрели текущее состояние переключателей SELinux для Apache с помощью команды **sestatus -b | grep httpd**. (fig. 3.4)



```
[root@kokuvshinova ~]# 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
```

Figure 3.4: Выполнение команды `sestatus -b | grep httpd`

5. Посмотрели статистику по политике с помощью команды **seinfo**.  
Определили, что множество пользователей = 8; ролей = 14; типов = 5002. (fig. 3.5)

```
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:                  133      Permissions:              454
Sensitivities:            1        Categories:              1024
Types:                    5002     Attributes:               254
Users:                    8         Roles:                    14
Booleans:                 347      Cond. Expr.:             381
Allow:                    63996    Neverallow:               0
Auditallow:               168      Dontaudit:               8417
Type_trans:               258486   Type_change:              87
Type_member:               35       Range_trans:             5960
Role allow:                38       Role_trans:              420
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:                  651
Netifcon:                 0        Nodecon:                  0
```

Figure 3.5: Статистика по политике

6. Определили тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды **ls -lZ /var/www**. (fig. 3.6)

```
[root@kokuvshinova ~]# 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 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 мая 16 15:10 html
[root@kokuvshinova ~]#
```

Figure 3.6: Выполнение команды **ls -lZ /var/www**

7. Необходимо было определить тип файлов, находящихся в директории /var/www/html, с помощью команды **ls -lZ /var/www/html**. Но в данной директории файлов не обнаружилось. (fig. 3.7)

```
[root@kokuvshinova ~]# ls -lZ /var/www/html
итого 0
```

Figure 3.7: Выполнение команды `ls -lZ /var/www/html`

8. Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html - только uesr. (fig. 3.8)

```
[root@kokuvshinova ~]# 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 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 16 15:10 html
[root@kokuvshinova ~]#
```

Figure 3.8: Выполнение команды `ls -lZ /var/www`

9. Создали от имени суперпользователя html-файл /var/www/html/test.html следующего содержания: (fig. 3.9)



The screenshot shows a text editor window with a title bar containing 'test.html' and the path '/var/www/html'. The editor has a menu bar with 'Открыть' (Open) and a '+' icon. The main text area contains three lines of HTML code:

```
1 <html>
2 <body> test </body>
3 </html>
```

Figure 3.9: Содержимое файла test.html

10. Проверили контекст созданного файла - httpd\_sys\_content\_t. (fig. 3.10)

```
[root@kokuvshinova ~]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 35 окт 10 17:37 /var/www/html/test.html
```

Figure 3.10: Контекст файла test.html

11. Обратились к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html` и убедились, что файл был успешно отображён. (fig. 3.11)

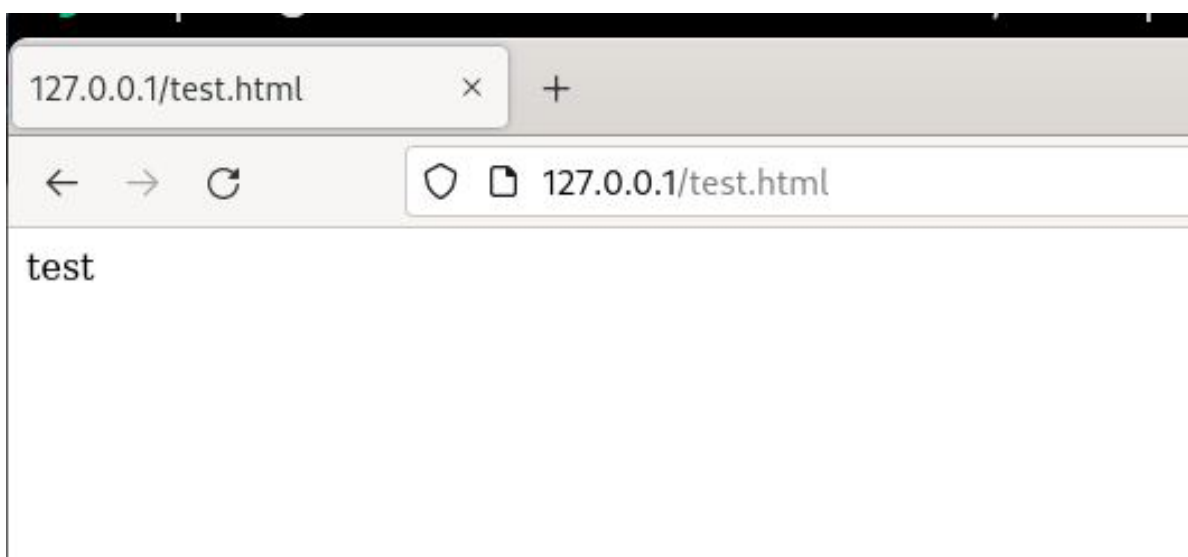


Figure 3.11: Обращение к файлу test.html через веб-сервер

12. Изучили справку `man httpd_selinux`. Тип файла `test.html` - контекст созданного файла - `httpd_sys_content_t`. (fig. 3.12)

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

Figure 3.12: Контекст файла test.html

13. Изменили контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`: `chcon -t samba_share_t /var/www/html/test.html` `ls -Z /var/www/html/test.html` И проверили, что контекст поменялся. (fig. 3.13)

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

Figure 3.13: Изменение контекста файла /var/www/html/test.html

14. Пробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. В результате получили ошибку. (fig. 3.14)

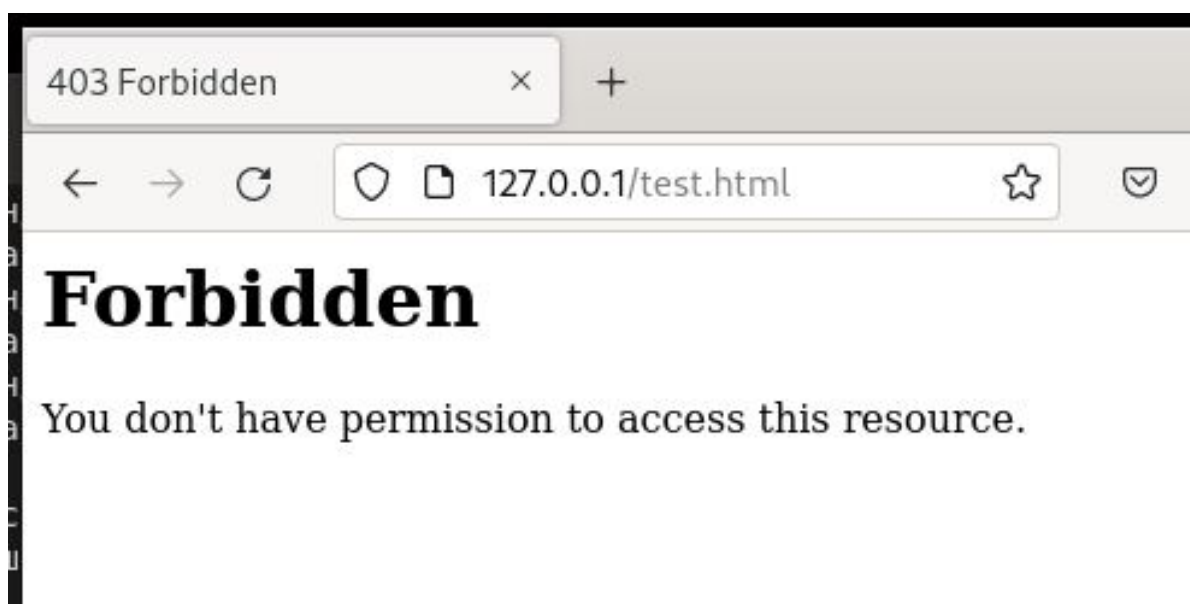


Figure 3.14: Обращение к файлу test.html через веб-сервер после изменения контекста

15. Проанализируем ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? `ls -l /var/www/html/test.html` Просмотрим log-файлы веб-сервера Apache и системный лог-файл: `tail /var/log/messages` В системе оказались запущенны процессы **setroubleshootd** и **audtd**. (fig. 3.15)



```
[root@kokuvshinova ~]# ls -l /var/www/html/test.html
-rw-r--r-- 1 root root 35 окт 10 17:37 /var/www/html/test.html
[root@kokuvshinova ~]# tail /var/log/messages
Oct 10 17:43:03 kokuvshinova setroubleshoot[40846]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/test.html.#012#012*****
Модуль restorecon предлагает (точность 92.2) *****#012#012Если вы хотите исправить метку.$TARGETЗнак PATH по умолчанию должен
быть httpd_sys_content_t#012То вы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за недостаточных разрешений для досту
па к родительскому каталогу, и в этом случае попробуйте соответствующим образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /v
ar/www/html/test.html#012#012***** Модуль public content предлагает (точность 7.83) *****#012#012Если вы хотите лечить test.html
как общедоступный контент#012То необходимо изменить метку test.html с public content t на public content rw t.#012Сделать#012# semanage fcontext -a
-t public content t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012***** Модуль catchall предлагает (точность 1.41
) *****#012#012Если вы считаете, что httpd должно быть разрешено getattr доступ к test.html file по умолчанию.#012То рекомен
дуется создать отчет об ошибке.#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, вып
олнив:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 10 17:43:03 kokuvshinova setroubleshoot[40846]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/test.html. Для выполнения
всех сообщений SELinux: sealert -l d5d733e3-d9b6-488f-8980-534db7e24dc2
Oct 10 17:43:03 kokuvshinova setroubleshoot[40846]: SELinux запрещает /usr/sbin/httpd доступ getattr к файл /var/www/html/test.html.#012#012*****
Модуль restorecon предлагает (точность 92.2) *****#012#012Если вы хотите исправить метку.$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 досту
па к родительскому каталогу, и в этом случае попробуйте соответствующим образом изменить следующую команду.#012Сделать#012# /sbin/restorecon -v /v
ar/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 рекомен
дуется создать отчет об ошибке.#012Чтобы разрешить доступ, можно создать локальный модуль политики.#012Сделать#012разрешить этот доступ сейчас, вып
олнив:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct 10 17:43:13 kokuvshinova systemd[1]: dbus-1.10-org.fedoraproject.SetroubleshootPrivileged@0.service: Main process exited, code=killed, status=
14/ALRM
Oct 10 17:43:13 kokuvshinova systemd[1]: dbus-1.10-org.fedoraproject.SetroubleshootPrivileged@0.service: Failed with result 'signal'.
Oct 10 17:43:13 kokuvshinova systemd[1]: dbus-1.10-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 2.230s CPU time.
Oct 10 17:43:13 kokuvshinova systemd[1]: dbus-1.10-org.fedoraproject.Setroubleshootd@0.service: Main process exited, code=killed, status=14/ALRM
Oct 10 17:43:13 kokuvshinova systemd[1]: dbus-1.10-org.fedoraproject.Setroubleshootd@0.service: Failed with result 'signal'.
Oct 10 17:43:13 kokuvshinova systemd[1]: dbus-1.10-org.fedoraproject.Setroubleshootd@0.service: Consumed 1.670s CPU time.
[root@kokuvshinova ~]#
```

Figure 3.15: Вывод команд `ls -l /var/www/html/test.html` и `tail /var/log/messages`

16. Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле `/etc/httpd/httpd.conf` находим строчку `Listen 80` и заменяем её на `Listen 81`. (fig. 3.16)



The screenshot shows a text editor window titled 'httpd.conf /etc/httpd/conf'. The file content is as follows:

```
44 # page for more information.
45 #
46 #Listen 12.34.56.78:80
47 Listen 81
48
49 #
50 # Dynamic Shared Object (DSO) Support
51 #
52 # To be able to use the functionality of a module which was built as a
```

Figure 3.16: Запуск веб-сервера Apache на прослушивание TCP-порта 81

17. Выполним перезапуск веб-сервера Apache. Произошёл сбой? Нет.
18. Проанализируем лог-файлы: `tail -nl /var/log/messages` Просмотрим файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log`. (fig. 3.17)

```
[root@kokuvshinova conf]# systemctl restart httpd
[root@kokuvshinova conf]# tail -n1 /var/log/messages
Oct 10 17:50:15 kokuvshinova httpd[41216]: Server configured, listening on: port 81
```

Figure 3.17: Перезапуск веб-сервера Apache

19. Выполним команду **semanage port -a -t http\_port\_t -p tcp 81**. Вылетает **ValueError** в связи с тем, что порт уже определен. После этого проверим список портов командой **semanage port -l | grep http\_port\_t** и убедимся, что порт 81 появился в списке. (fig. 3.18)

```
[root@kokuvshinova conf]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@kokuvshinova conf]# 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
```

Figure 3.18: Проверка установления 81 порта tcp

20. Попробуем запустить веб-сервер Apache ещё раз. (fig. 3.19)

```
[root@kokuvshinova conf]# systemctl restart httpd
[root@kokuvshinova conf]#
```

Figure 3.19: Перезапуск веб-сервера Apache

21. Вернули контекст **httpd\_sys\_content\_t** к файлу **/var/www/html/test.html**: **chcon -t httpd\_sys\_content\_t /var/www/html/test.html** (fig. 3.20)

```
[root@kokuvshinova conf]# systemctl restart httpd
[root@kokuvshinova conf]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@kokuvshinova conf]# ls -Z /var/www/
cgi-bin/ html/
[root@kokuvshinova conf]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@kokuvshinova conf]#
```

Figure 3.20: Возвращение контекста **httpd\_sys\_content\_t** к файлу **test.html**

После этого пробуем получить доступ к файлу через веб-сервер, введя в браузере адрес **http://127.0.0.1:81/test.html**. В результате увидели содержимое файла — слово «test». (fig. 3.21)

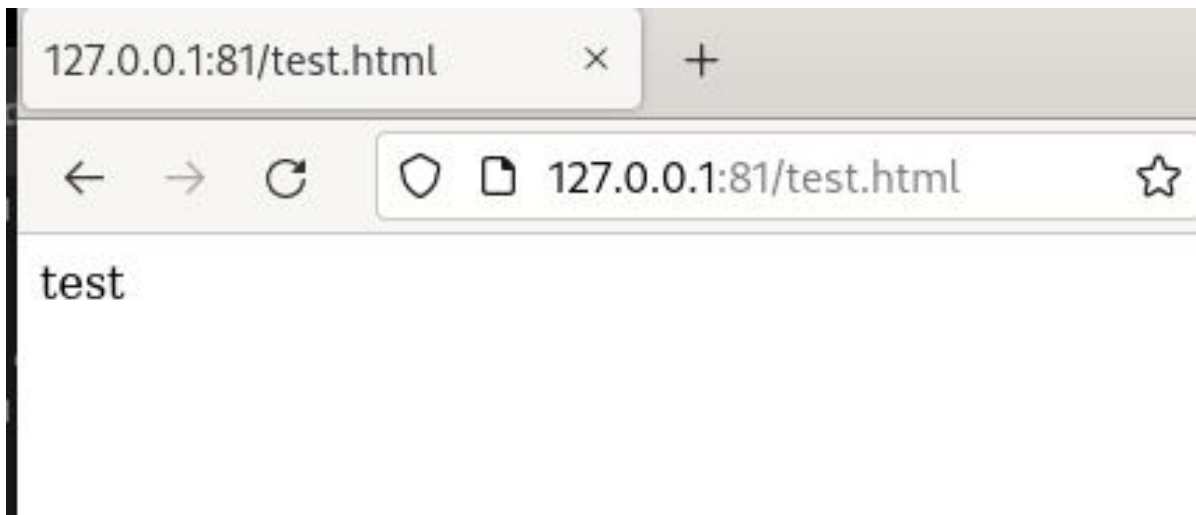


Figure 3.21: Обращение к файлу test.html через веб-сервер

22. Исправим обратно конфигурационный файл apache, вернув Listen 80. (fig. 3.22)

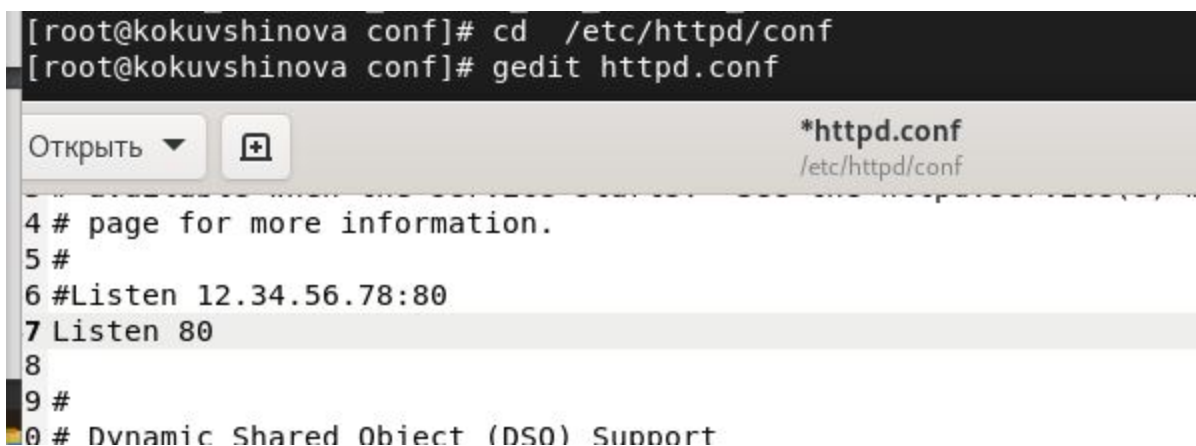


Figure 3.22: Исправление конфигурационного файла apache

23. Удалим привязку `http_port_t` к 81 порту: **`semanage port -d -t http_port_t -p tcp 81`** и проверим, что порт 81 удалён. Данная команда не была выполнена. (fig. 3.23)

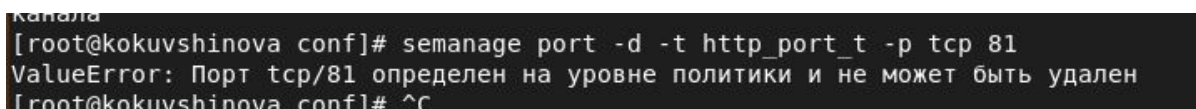


Figure 3.23: Удаление привязки `http_port_t` к 81 порту



24. Удалим файл /var/www/html/test.html: **rm /var/www/html/test.html.**  
(fig. 3.24)

A terminal window with a dark background. The prompt is [root@kokuvshinova conf]#. The command entered is rm /var/www/html/test.html. The output is rm: удалить обычный файл '/var/www/html/test.html'? y.

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

Figure 3.24: Удаление файла test.html

## 4 Вывод

В ходе выполнения лабораторной работы мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.

## 5 Библиография

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Мандатное разграничение прав в Linux [Текст] / Кулябов Д. С., Королькова А. В., Геворкян М. Н. - Москва: - 5 с. [^1]: Мандатное разграничение прав в Linux.
2. Справочник 70 основных команд Linux: полное описание с примерами (<https://eternalhost.net/blog/sozdanie-saytov/osnovnye-komandy-linux>)