

# **Лабораторная работа №6**

**Мандатное разграничение прав в Linux**

Роман Владимирович Иванов

# Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	21
5	Список литературы	22

# Список иллюстраций

3.1	Установка Apache . . . . .	7
3.2	Внесение информации в конфигурационный файл . . . . .	7
3.3	Чтение конфигурационного файла . . . . .	8
3.4	Отключение пакетного фильтра . . . . .	8
3.5	Проверка режима работы SELinux . . . . .	9
3.6	Проверка работы веб-сервера . . . . .	9
3.7	Поиск веб-сервера Apache и определение его контекста безопасности	10
3.8	Текущее состояние переключателей SELinux для Apache . . . . .	11
3.9	Статистика по политике . . . . .	12
3.10	Определение типов файлов и поддиректорий, находящихся в директории /var/www . . . . .	12
3.11	Определение типов файлов и поддиректорий, находящихся в директории /var/www/html . . . . .	12
3.12	Пользователи, которым разрешено создание файлов в директории	13
3.13	html-файл и его содержимое . . . . .	13
3.14	Контекст html-файл . . . . .	14
3.15	Обращение к файлу через браузер . . . . .	14
3.16	Выяснение контекста файла . . . . .	14
3.17	Изменение контекста файла . . . . .	15
3.18	Попытка получить доступ к файлу через веб-сервер . . . . .	15
3.19	Просмотр системного лог-файла . . . . .	16
3.20	Изменение строки файла . . . . .	16
3.21	Просмотр файла /var/log/http/error_log . . . . .	17
3.22	Просмотр файла /var/log/http/access_log . . . . .	17
3.23	Просмотр файла /var/log/audit/audit.log . . . . .	18
3.24	Просмотр портов . . . . .	18
3.25	Возвращение исходного контекста . . . . .	18
3.26	Получение доступа к файлу через веб-сервер . . . . .	19
3.27	Возвращение строки Listen 80 . . . . .	20
3.28	Попытка удаления привязки http_port_t к 81 порту . . . . .	20
3.29	Удаление файла /var/www/html/test.html . . . . .	20

## Список таблиц

# 1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. [1]

Проверить работу SELinx на практике совместно с веб-сервером Apache.

## 2 Задание

1. Подготовить лабораторный стенд и ознакомиться с методическими рекомендациями.
2. С помощью различных примеров ознакомиться с работой SELinux и веб-сервисом Apache.

### 3 Выполнение лабораторной работы

1. Подготовил лабораторный стенд и ознакомился с методическими рекомендациями.

Предварительно установил веб-сервис Apache с помощью команды `yum install httpd` (рис - @fig:001).

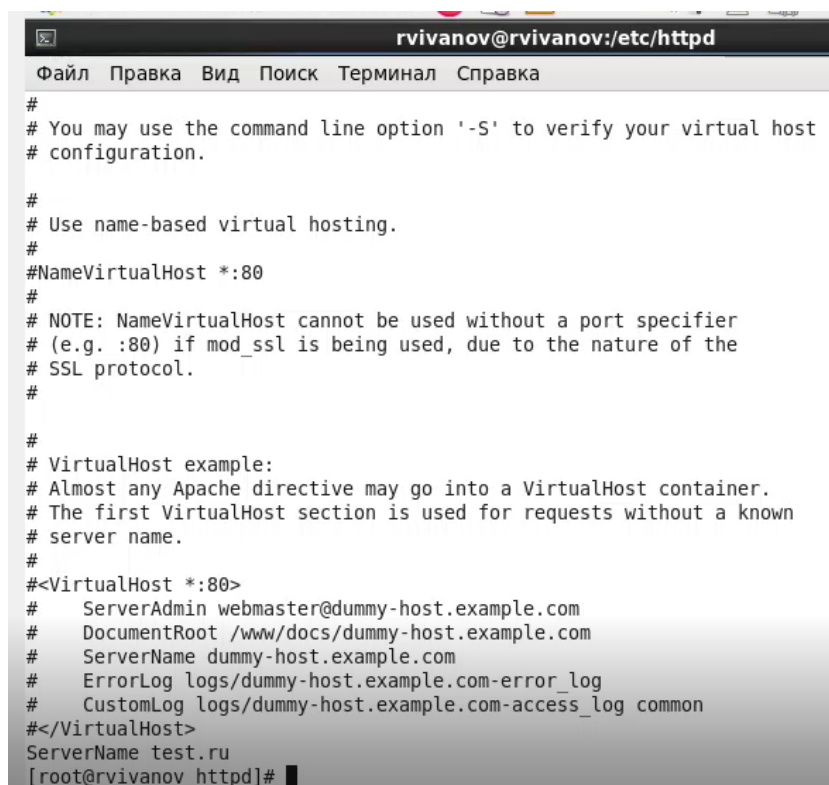
```
[root@rvivanov Рабочий стол]# yum install httpd
Загружены модули: fastestmirror, refresh-packagekit, security
Подготовка к установке
Determining fastest mirrors
base | 3.7 kB | 00:00
extras | 3.3 kB | 00:00
updates | 3.4 kB | 00:00
Пакет httpd-2.2.15-69.el6.centos.i686 уже установлен, и это последняя версия.
Выполнять нечего
[root@rvivanov Рабочий стол]#
```

Рис. 3.1: Установка Apache

В конфигурационном файле `/etc/httpd/httpd.conf` задал параметр `ServerName: ServerName test.ru`. Это делается для того, чтобы при запуске веб-сервиса не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе (рис - @fig:002 и @fig:003).

```
-rw-r--r--. 1 root root 299 Фев 19 2018 welcome.conf
[root@rvivanov conf.d]# cd ..
[root@rvivanov httpd]# echo "ServerName test.ru" >> /etc/httpd/conf/httpd.conf
```

Рис. 3.2: Внесение информации в конфигурационный файл



```
rvivanov@rvivanov:/etc/httpd
Файл  Правка  Вид  Поиск  Терминал  Справка
#
# You may use the command line option '-S' to verify your virtual host
# configuration.
#
# Use name-based virtual hosting.
#
#NameVirtualHost *:80
#
# NOTE: NameVirtualHost cannot be used without a port specifier
# (e.g. :80) if mod_ssl is being used, due to the nature of the
# SSL protocol.
#
#
# VirtualHost example:
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for requests without a known
# server name.
#
#<VirtualHost *:80>
#   ServerAdmin webmaster@dummy-host.example.com
#   DocumentRoot /www/docs/dummy-host.example.com
#   ServerName dummy-host.example.com
#   ErrorLog logs/dummy-host.example.com-error_log
#   CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>
ServerName test.ru
[root@rvivanov httpd]#
```

Рис. 3.3: Чтение конфигурационного файла

Также отключил пакетный фильтр (рис - @fig:004).

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

Рис. 3.4: Отключение пакетного фильтра

2. С помощью различных примеров ознакомился с работой SELinux и веб-сервисом Apache.

Вошел в систему с полученными учетными данными и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus` (рис - @fig:005).



```
[root@rvivanov httpd]# getenforce
Enforcing
[root@rvivanov httpd]# sestatus
SELinux status:                enabled
SELinuxfs mount:              /selinux
Current mode:                  enforcing
Mode from config file:         enforcing
Policy version:                24
Policy from config file:       targeted
[root@rvivanov httpd]# █
```

Рис. 3.5: Проверка режима работы SELinux

Обратится с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедился, что последний работает с помощью команды `/etc/rc.d/init.d/httpd status`, предварительно запустив его с помощью команды `/etc/rc.d/init.d/httpd start` (рис - @fig:006).

```
[root@rvivanov httpd]# service httpd status
httpd остановлен
[root@rvivanov httpd]# /etc/rc.d/init.d/httpd status
httpd остановлен
[root@rvivanov httpd]# /etc/rc.d/init.d/httpd start
Запускается httpd: [ OK ]
[root@rvivanov httpd]# /etc/rc.d/init.d/httpd status
httpd (pid 2433) выполняется...
[root@rvivanov httpd]# █
```

Рис. 3.6: Проверка работы веб-сервера

Нашел веб-сервер Apache в списке процессов и определил его контекст безопасности с помощью команды `ps auxZ | grep httpd` (рис - @fig:007).

```
[root@rvivanov httpd]# ps auxZ | grep httpd
unconfined_u:system_r:httpd_t:s0 root      2433  0.0  0.3 11644 3352 ?        Ss   12:41   0:00
/usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache    2436  0.0  0.2 11644 2180 ?        S    12:41   0:00
/usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache    2437  0.0  0.2 11644 2180 ?        S    12:41   0:00
/usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache    2438  0.0  0.2 11644 2208 ?        S    12:41   0:00
/usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache    2439  0.0  0.2 11644 2180 ?        S    12:41   0:00
/usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache    2440  0.0  0.2 11644 2180 ?        S    12:41   0:00
/usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache    2441  0.0  0.2 11644 2180 ?        S    12:41   0:00
/usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache    2442  0.0  0.2 11644 2180 ?        S    12:41   0:00
/usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache    2443  0.0  0.2 11644 2180 ?        S    12:41   0:00
/usr/sbin/httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 2452  0.0  0.0 4444 808 pts/0 S+   12:42
0:00 grep httpd
[root@rvivanov httpd]#
```

Рис. 3.7: Поиск веб-сервера Apache и определение его контекста безопасности

Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b` (рис - @fig:008). Многие из них находятся в положении “off”.

```

Without options, show SELinux status.
[root@rvivanov httpd]# sestatus -b
SELinux status:                enabled
SELinuxfs mount:              /selinux
Current mode:                  enforcing
Mode from config file:         enforcing
Policy version:                24
Policy from config file:       targeted

Policy booleans:
abrt_anon_write                off
abrt_handle_event              off
allow_console_login            on
allow_cvs_read_shadow          off
allow_daemons_dump_core       on
allow_daemons_use_tcp_wrapper off
allow_daemons_use_tty         on
allow_domain_fd_use            on
allow_execheap                 off
allow_execmem                  on
allow_execmod                  on
allow_execstack                on
allow_ftpd_anon_write          off
allow_ftpd_full_access         off
allow_ftpd_use_cifs            off
allow_ftpd_use_nfs             off
allow_gssd_read_tmp            on

```

Рис. 3.8: Текущее состояние переключателей SELinux для Apache

Посмотрел статистику по политике с помощью команды `seinfo`, а также определил множество пользователей, ролей, типов (рис - @fig:009).

```
[root@rvivanov httpd]# seinfo

Statistics for policy file: /etc/selinux/targeted/policy/policy.24
Policy Version & Type: v.24 (binary, mls)

Classes:          81      Permissions:      238
Sensitivities:    1       Categories:      1024
Types:            3920    Attributes:       295
Users:            9       Roles:           12
Booleans:         237    Cond. Expr.:     277
Allow:            323336  Neverallow:      0
Auditallow:       141    Dontaudit:       274738
Type_trans:       42431  Type_change:     38
Type_member:      48     Role_allow:      19
Role_trans:       386    Range_trans:     6258
Constraints:      90     Validatetrans:   0
Initial SIDs:     27     Fs_use:          23
Genfscon:         84     Portcon:         474
Netifcon:         0      Nodecon:         0
Permissives:     90     Polcap:          2
```

Рис. 3.9: Статистика по политике

Определил тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www` (рис - @fig:010).

```
[root@rvivanov httpd]# 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 error
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 icons
[root@rvivanov httpd]#
```

Рис. 3.10: Определение типов файлов и поддиректорий, находящихся в директории /var/www

Определил тип файлов, находящихся в директории /var/www/html с помощью команды `ls -lZ /var/www/html` (рис - @fig:011).

```
[root@rvivanov httpd]# ls -lZ /var/www/html
[root@rvivanov httpd]#
```

Рис. 3.11: Определение типов файлов и поддиректорий, находящихся в директории /var/www/html

Консоль ничего не выводит, поскольку директория пуста.

Определил круг пользователей, которым разрешено создание файлов в директории /var/www/html (рис - @fig:012).

```
[root@rvivanov httpd]# ls -l /var/www
итого 16
drwxr-xr-x. 2 root root 4096 Июн 19 2018 cgi-bin
drwxr-xr-x. 3 root root 4096 Сен 18 15:25 error
drwxr-xr-x. 2 root root 4096 Июн 19 2018 html
drwxr-xr-x. 3 root root 4096 Сен 18 15:25 icons
[root@rvivanov httpd]#
```

Рис. 3.12: Пользователи, которым разрешено создание файлов в директории

Создал от имени суперпользователя html-файл /var/www/html/test.html следующего содержания (рис - @fig:013):

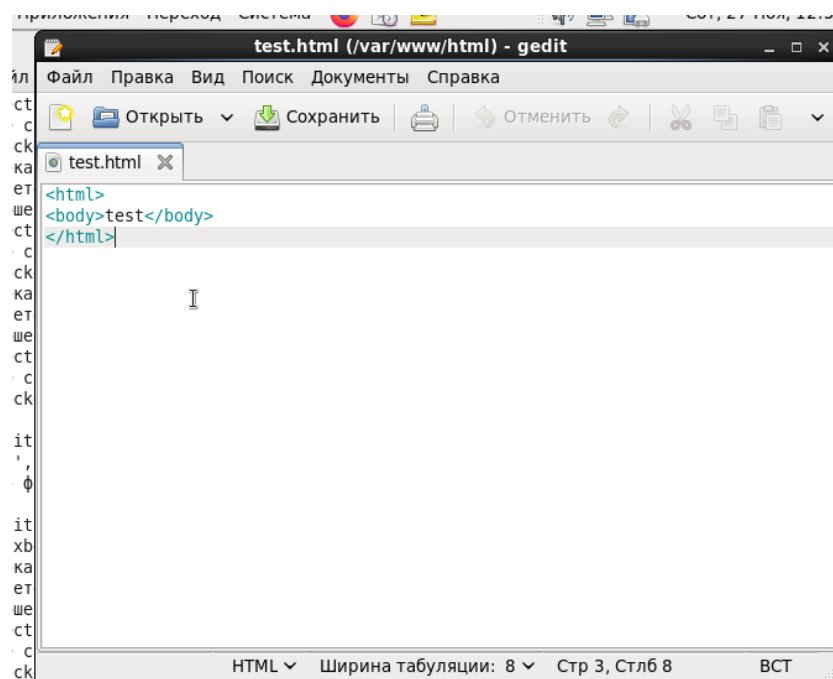


Рис. 3.13: html-файл и его содержимое

Проверил контекст созданного мною файла (рис - @fig:014):

```
[root@rvivanov httpd]# 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
[root@rvivanov httpd]#
```

Рис. 3.14: Контекст html-файл

Обратился к файлу через веб-сервис, введя в браузере адрес `http://127.0.0.1/test.html` (рис - @fig:015):

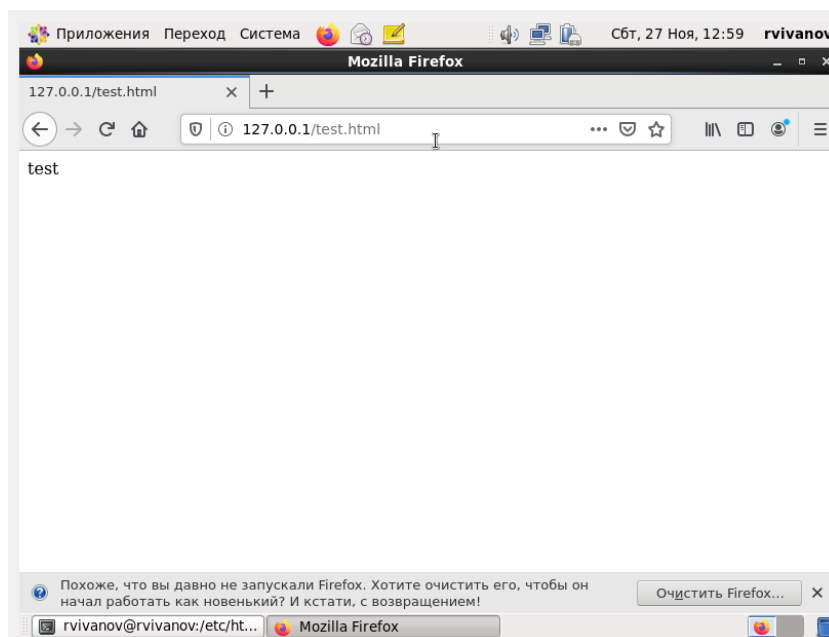


Рис. 3.15: Обращение к файлу через браузер

Проверил контекст файла с помощью команды `ls -Z /var/www/html/test.html` (рис - @fig:016).

```
[root@rvivanov httpd]# 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
[root@rvivanov httpd]#
```

Рис. 3.16: Выяснение контекста файла

Изменил контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t` (рис - @fig:017).

```
[root@rvivanov httpd]# chcon -t samba_share_t /var/www/html/test.html
[root@rvivanov httpd]# 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@rvivanov httpd]#
```

Рис. 3.17: Изменение контекста файла

Попробовал еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получил ошибку (рис - @fig:018).



Рис. 3.18: Попытка получить доступ к файлу через веб-сервер

Проанализировал ситуацию. Просмотрел log-файлы веб-сервера Apache, а также посмотрел системный лог-файл с помощью команды `tail /var/log/messages` (рис - @fig:019).

```
[root@rvivanov httpd]# tail /var/log/messages
Nov 27 13:06:40 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (16
)
Nov 27 13:06:40 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (11
)
Nov 27 13:06:40 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (12
)
Nov 27 13:06:40 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (13
)
Nov 27 13:06:40 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (14
)
Nov 27 13:06:40 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (15
)
Nov 27 13:06:40 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (16
)
Nov 27 13:06:40 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (17
)
Nov 27 13:06:40 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (18
)
Nov 27 13:06:40 rvivanov kernel: audit: freed 18 contexts
[root@rvivanov httpd]# █
```

Рис. 3.19: Просмотр системного лог-файла

Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле /etc/httpd/httpd.conf нашел строчку Listen 80 и заменил ее на Listen 81 (рис - @fig:020).

```
[root@rvivanov conf]# tail -l /var/log/messages
Nov 27 13:10:31 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (16
)
Nov 27 13:10:31 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (17
)
Nov 27 13:10:31 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (18
)
Nov 27 13:10:31 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (19
)
Nov 27 13:10:31 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (20
)
Nov 27 13:10:31 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (21
)
Nov 27 13:10:31 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (22
)
Nov 27 13:10:31 rvivanov kernel: audit: freed 22 contexts
Nov 27 13:17:08 rvivanov kernel: audit(:0): major=1 name_count=0: freeing multiple contexts (1)
Nov 27 13:17:08 rvivanov kernel: audit(:0): major=355 name_count=0: freeing multiple contexts (2)
[root@rvivanov conf]# █
```

Рис. 3.20: Изменение строки файла

Просмотрел файл /var/log/http/error\_log (рис - @fig:021).



```
[root@rvivanov httpd]# cat /var/log/httpd/error_log
[Sat Nov 27 12:41:31 2021] [notice] SELinux policy enabled; httpd running as context unconfined_u
:system_r:httpd_t:s0
[Sat Nov 27 12:41:31 2021] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Nov 27 12:41:31 2021] [notice] Digest: generating secret for digest authentication ...
[Sat Nov 27 12:41:31 2021] [notice] Digest: done
[Sat Nov 27 12:41:31 2021] [notice] Apache/2.2.15 (Unix) DAV/2 configured -- resuming normal operations
[Sat Nov 27 12:41:31 2021] [warn] ./mod_dnssd.c: No services found to register
[Sat Nov 27 12:59:35 2021] [error] [client 127.0.0.1] File does not exist: /var/www/html/favicon.
ico
[Sat Nov 27 13:06:48 2021] [error] [client 127.0.0.1] (13)Permission denied: access to /test.html
denied
[Sat Nov 27 13:17:10 2021] [error] [client 127.0.0.1] (13)Permission denied: access to /test.html
denied
[Sat Nov 27 13:17:11 2021] [error] [client 127.0.0.1] (13)Permission denied: access to /test.html
denied
[Sat Nov 27 13:17:11 2021] [error] [client 127.0.0.1] (13)Permission denied: access to /test.html
denied
[Sat Nov 27 13:23:12 2021] [error] [client 127.0.0.1] (13)Permission denied: access to /test.html
denied
[Sat Nov 27 13:23:38 2021] [error] [client 127.0.0.1] (13)Permission denied: access to /test.html
denied
[root@rvivanov httpd]# █
```

Рис. 3.21: Просмотр файла /var/log/http/error\_log

Просмотрел файл /var/log/http/access\_log (рис - @fig:022).

```
[root@rvivanov httpd]# cat /var/log/httpd/access_log
127.0.0.1 - - [27/Nov/2021:12:59:34 +0300] "GET /test.html HTTP/1.1" 200 33 "-" Mozilla/5.0 (X11
; Linux i686; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [27/Nov/2021:12:59:35 +0300] "GET /favicon.ico HTTP/1.1" 404 284 "-" Mozilla/5.0 (
X11; Linux i686; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [27/Nov/2021:13:06:48 +0300] "GET /test.html HTTP/1.1" 403 286 "-" Mozilla/5.0 (X1
l; Linux i686; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [27/Nov/2021:13:17:10 +0300] "GET /test.html HTTP/1.1" 403 286 "-" Mozilla/5.0 (X1
l; Linux i686; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [27/Nov/2021:13:17:11 +0300] "GET /test.html HTTP/1.1" 403 286 "-" Mozilla/5.0 (X1
l; Linux i686; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [27/Nov/2021:13:17:11 +0300] "GET /test.html HTTP/1.1" 403 286 "-" Mozilla/5.0 (X1
l; Linux i686; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [27/Nov/2021:13:23:12 +0300] "GET /test.html HTTP/1.1" 403 286 "-" Mozilla/5.0 (X1
l; Linux i686; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [27/Nov/2021:13:23:38 +0300] "GET /test.html HTTP/1.1" 403 286 "-" Mozilla/5.0 (X1
l; Linux i686; rv:78.0) Gecko/20100101 Firefox/78.0"
[root@rvivanov httpd]# █
```

Рис. 3.22: Просмотр файла /var/log/http/access\_log

Просмотрел файл var/log/audit/audit.log (рис - @fig:023).

```
type=AVC msg=audit(1638008592.381:65): avc: denied { getattr } for pid=2439 comm="httpd" path=
"/var/www/html/test.html" dev=dm-0 ino=2224323 scontext=unconfined_u:system_r:httpd_t:s0 tcontext
=unconfined_u:object_r:samba_share_t:s0 tclass=file
type=SYSCALL msg=audit(1638008592.381:65): arch=40000003 syscall=195 success=no exit=-13 a0=14b2c
e8 a1=bfa49180 a2=7faff4 a3=8170 items=0 ppid=2433 pid=2439 auid=500 uid=48 gid=48 euid=48 suid=4
8 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=1 comm="httpd" exe="/usr/sbin/httpd" subj=unco
nfigined u:system_r:httpd_t:s0 key=(null)
type=AVC msg=audit(1638008592.381:66): avc: denied { getattr } for pid=2439 comm="httpd" path=
"/var/www/html/test.html" dev=dm-0 ino=2224323 scontext=unconfined_u:system_r:httpd_t:s0 tcontext
=unconfined_u:object_r:samba_share_t:s0 tclass=file
type=SYSCALL msg=audit(1638008592.381:66): arch=40000003 syscall=196 success=no exit=-13 a0=14b2d
80 a1=bfa49180 a2=7faff4 a3=2008171 items=0 ppid=2433 pid=2439 auid=500 uid=48 gid=48 euid=48 sui
d=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=1 comm="httpd" exe="/usr/sbin/httpd" subj=u
nconfined u:system_r:httpd_t:s0 key=(null)
type=AVC msg=audit(1638008618.507:67): avc: denied { getattr } for pid=2437 comm="httpd" path=
"/var/www/html/test.html" dev=dm-0 ino=2224323 scontext=unconfined_u:system_r:httpd_t:s0 tcontext
=unconfined_u:object_r:samba_share_t:s0 tclass=file
type=SYSCALL msg=audit(1638008618.507:67): arch=40000003 syscall=195 success=no exit=-13 a0=14b0c
e0 a1=bfa49180 a2=7faff4 a3=8170 items=0 ppid=2433 pid=2437 auid=500 uid=48 gid=48 euid=48 suid=4
8 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=1 comm="httpd" exe="/usr/sbin/httpd" subj=unco
nfigined u:system_r:httpd_t:s0 key=(null)
type=AVC msg=audit(1638008618.507:68): avc: denied { getattr } for pid=2437 comm="httpd" path=
"/var/www/html/test.html" dev=dm-0 ino=2224323 scontext=unconfined_u:system_r:httpd_t:s0 tcontext
=unconfined_u:object_r:samba_share_t:s0 tclass=file
type=SYSCALL msg=audit(1638008618.507:68): arch=40000003 syscall=196 success=no exit=-13 a0=14b0d
78 a1=bfa49180 a2=7faff4 a3=2008171 items=0 ppid=2433 pid=2437 auid=500 uid=48 gid=48 euid=48 sui
d=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=1 comm="httpd" exe="/usr/sbin/httpd" subj=u
nconfined u:system_r:httpd_t:s0 key=(null)
[root@rvivanov httpd]# cat /var/log/audit/audit.log
```

Рис. 3.23: Просмотр файла /var/log/audit/audit.log

Выполнил команду `semanage port -a -t http_port_t -p tcp 81`. После этого прове-  
рил список портов командой `semanage port -l | grep http_port_t` (рис - @fig:024).  
Убедился, что порт 81 появился в списке.

```
[root@rvivanov httpd]# semanage port -a -t http_port_t -p tcp 81
/usr/sbin/semanage: Порт tcp/81 уже определен
[root@rvivanov httpd]# 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
```

Рис. 3.24: Просмотр портов

Вернул контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html` с  
помощью команды `chcon -t httpd_sys_content_t /var/www/html/test.html` (рис -  
@fig:025). После этого попробовал получить доступ к файлу через веб-сервер,  
введя в браузере адрес `http://127.0.0.1:81/test.html` (рис - @fig:026).

```
[root@rvivanov httpd]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@rvivanov httpd]#
```

Рис. 3.25: Возвращение исходного контекста

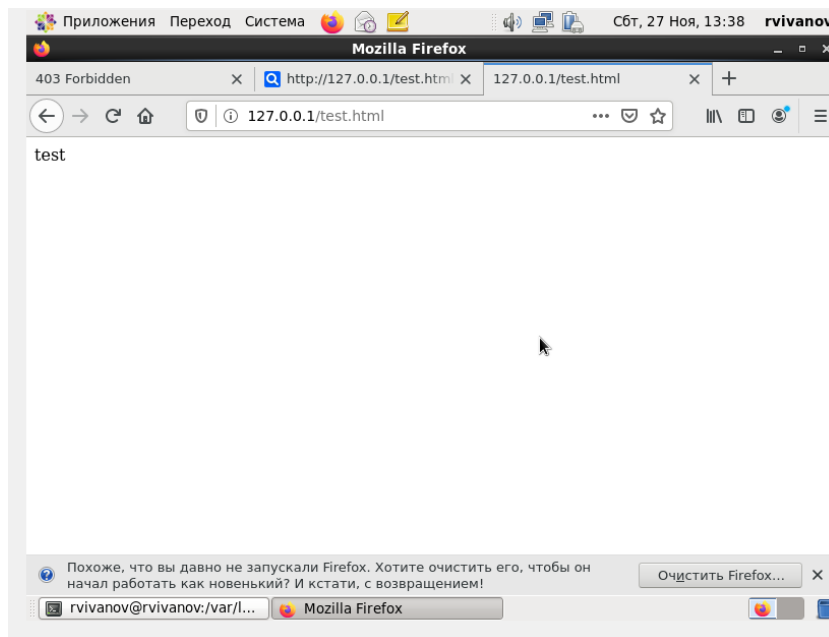


Рис. 3.26: Получение доступа к файлу через веб-сервер

Исправил обратно конфигурационный файл apache, вернув Listen 80 (рис - @fig:027).

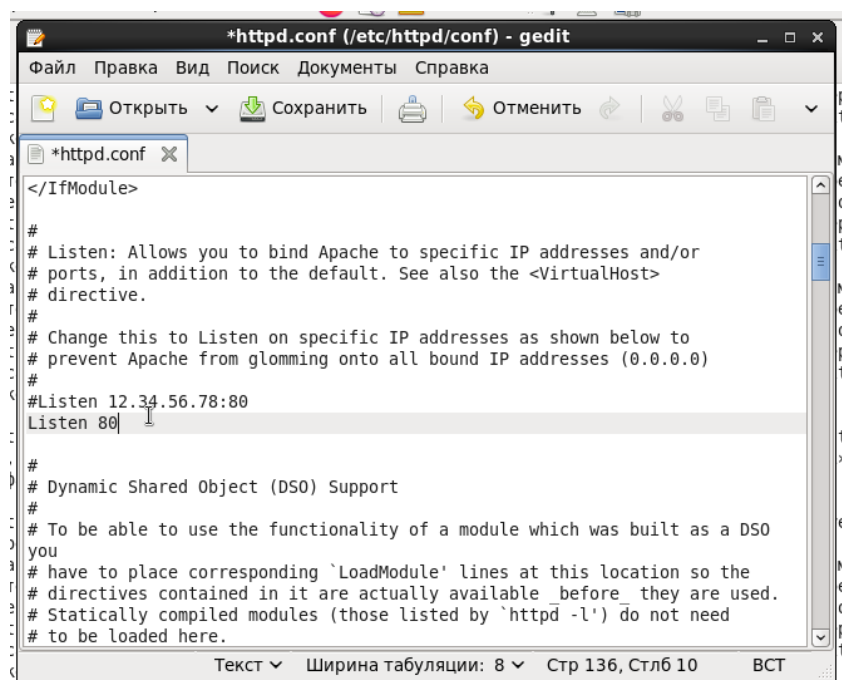


Рис. 3.27: Возвращение строки Listen 80

Попытался удалить привязку http\_port\_t к 81 порту (рис - @fig:028).

```
httpd (pid 2433) выполняется...
[root@rvivanov conf]# semanage port -d -t http_port_t -p tcp 81
/usr/sbin/semanage: Порт tcp/81 определен на уровне политики и не может быть удален
```

Рис. 3.28: Попытка удаления привязки http\_port\_t к 81 порту

Удалил файл /var/www/html/test.html (рис - @fig:029).

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

Рис. 3.29: Удаление файла /var/www/html/test.html

## 4 Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux.

Проверил работу SELinux на практике совместно с веб-сервером Apache.

## 5 Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 6. Мандатное разграничение прав в Linux.