

# РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

## ОТЧЕТ

### ПО ЛАБОРАТОРНОЙ РАБОТЕ № 6

*Дисциплина: Основы информационной безопасности*

*Название работы: Мандатное разграничение прав в Linux*

Студент: Степанов Виктор

Группа: НПМбд-02-18

МОСКВА

2021 г.

## Цель работы

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

## Подготовка лабораторного стенда

1. Установим/обновим (за суперпользователя) веб-сервер Apache с помощью команды ***yum install httpd*** (Рис. 1)

```
Файл  Правка  Вид  Поиск  Терминал  Справка
(2/2): httpd-tools-2.2.15-69.el6.centos.i686.rpm | 81 kB  00:00
-----
Общий размер                               508 kB/s | 925 kB  00:01
Запуск rpm_check_debug
Проверяем сценарий
Проверка сценария прошла успешно
Запускается сценарий
  Обновление : httpd-tools-2.2.15-69.el6.centos.i686      1/4
  Обновление : httpd-2.2.15-69.el6.centos.i686           2/4
  Очистка     : httpd-2.2.15-39.el6.centos.i686           3/4
  Очистка     : httpd-tools-2.2.15-39.el6.centos.i686     4/4
  Verifying   : httpd-tools-2.2.15-69.el6.centos.i686     1/4
  Verifying   : httpd-2.2.15-69.el6.centos.i686           2/4
  Verifying   : httpd-2.2.15-39.el6.centos.i686           3/4
  Verifying   : httpd-tools-2.2.15-39.el6.centos.i686     4/4

Обновлено:
  httpd.i686 0:2.2.15-69.el6.centos

Зависимости обновлены:
  httpd-tools.i686 0:2.2.15-69.el6.centos

Готово!
[root@atoev Guest]#
```

Рис. 1

2. В конфигурационном файле ***/etc/httpd/httpd.conf*** зададим параметр **ServerName**: ***ServerName test.ru*** чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе. (Рис. 2)

```
Файл  Правка  Вид  Поиск  Терминал  Справка
GNU nano 2.0.9      Файл: /etc/httpd/conf/httpd.conf

ServerAdmin root@localhost

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work. See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
#ServerName test.ru
#
# UseCanonicalName: Determines how Apache constructs self-referencing
# URLs and the SERVER_NAME and SERVER_PORT variables.

^G Помощь      ^O Записать   ^R ЧитФайл   ^Y ПредСтр   ^K Вырезать  ^C ТекПозиц
^X Выход      ^J Выводить  ^W Поиск     ^V СледСтр   ^U ОтмВырезк ^T Словарь
```

Рис. 2

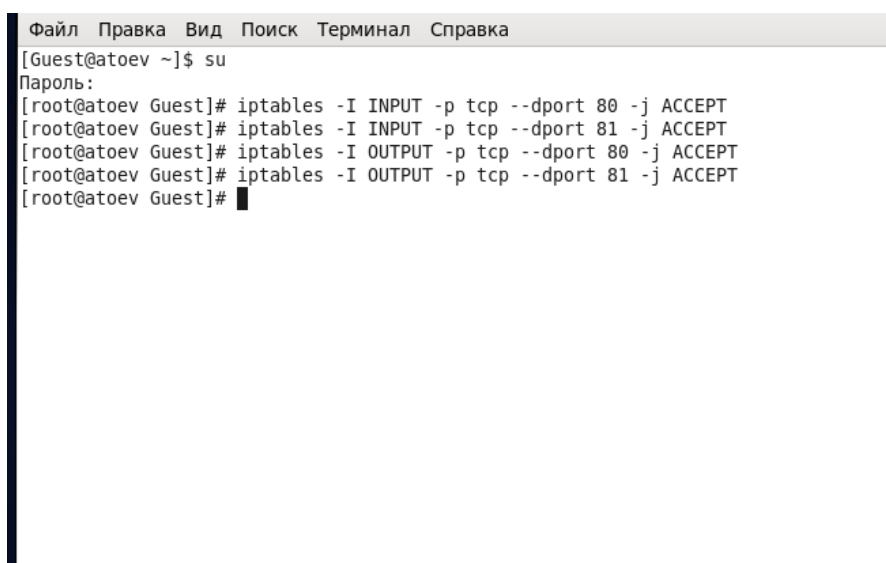
3. Необходимо проследить, чтобы пакетный фильтр был отключен или в своей рабочей конфигурации позволял подключаться к 80-му и 81-му портам протокола tcp. Добавим разрешающие правила с помощью команд (Рис. 3):

***iptables -I INPUT -p tcp --dport 80 -j ACCEPT***

***iptables -I INPUT -p tcp --dport 81 -j ACCEPT***

***iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT***

***iptables -I OUTPUT -p tcp --sport 81 -j ACCEPT***



```
Файл Правка Вид Поиск Терминал Справка
[Guest@atoev ~]$ su
Пароль:
[root@atoev Guest]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@atoev Guest]# iptables -I INPUT -p tcp --dport 81 -j ACCEPT
[root@atoev Guest]# iptables -I OUTPUT -p tcp --dport 80 -j ACCEPT
[root@atoev Guest]# iptables -I OUTPUT -p tcp --dport 81 -j ACCEPT
[root@atoev Guest]#
```

Рис. 3

Можно также отключить фильтр командами:

***iptables -F***

***iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT***

### Порядок выполнения работы

1. Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted с помощью команд *getenforce* и *sestatus* (Рис. 4)

```
Файл  Правка  Вид  Поиск  Терминал  Справка
[Guest@atoev ~]$ su
Пароль:
[root@atoev Guest]# getenforce
Enforcing
[root@atoev Guest]# sestatus
SELinux status:                enabled
SELinuxfs mount:              /selinux
Current mode:                  enforcing
Mode from config file:        enforcing
Policy version:                24
Policy from config file:      targeted
[root@atoev Guest]# █
```

Рис. 4

2. Обратимся к веб-серверу, запущенному на нашем компьютере, и убедимся, что последний работает: *service httpd status* (Рис. 5)

```
Файл  Правка  Вид  Поиск  Терминал  Справка
[Guest@atoev ~]$ su
Пароль:
[root@atoev Guest]# service httpd status
httpd остановлен
[root@atoev Guest]# service httpd start
Запускается httpd: httpd: apr_sockaddr_info_get() failed for atoev.localdomain
httpd: Could not reliably determine the server's fully qualified domain name, us
ing 127.0.0.1 for ServerName
[ OK ]
[root@atoev Guest]# service httpd status
httpd (pid 31620) выполняется...
[root@atoev Guest]# █
```

Рис. 5

3. Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности, используем команду *ps auxZ | grep httpd* (Рис. 6)

```
Файл Правка Вид Поиск Терминал Справка
[root@atoev Guest]# service httpd status
httpd (pid 31620) выполняется...
[root@atoev Guest]# ps auxZ | grep httpd
unconfined_u:system_r:httpd_t:s0 root      31620  0.1  0.3 11852  3540 ?        S
s  21:47  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  31623  0.0  0.2 11852  2228 ?        S
21:47  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  31624  0.0  0.2 11852  2204 ?        S
21:47  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  31625  0.0  0.2 11852  2204 ?        S
21:47  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  31626  0.0  0.2 11852  2204 ?        S
21:47  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  31627  0.0  0.2 11852  2204 ?        S
21:47  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  31628  0.0  0.2 11852  2204 ?        S
21:47  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  31629  0.0  0.2 11852  2204 ?        S
21:47  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  31630  0.0  0.2 11852  2204 ?        S
21:47  0:00 /usr/sbin/httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 31654 5.0  0.0 4376 7
96 pts/0 S+ 21:50  0:00 grep httpd
[root@atoev Guest]#
```

Рис. 6

4. Посмотрим текущее состояние переключателей SELinux для Apache с помощью команды *sestatus -b | grep httpd* (Рис. 7)

```
Файл Правка Вид Поиск Терминал Справка
[root@atoev Guest]# sestatus -b | grep httpd
allow_httpd_anon_write      off
allow_httpd_mod_auth_ntlm_winbind off
allow_httpd_mod_auth_pam    off
allow_httpd_sys_script_anon_write off
httpd_builtin_scripting     on
httpd_can_check_spam        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_avaahi           on
httpd_dbus_sssd             off
httpd_enable_cgi            on
httpd_enable_ftp_server     off
httpd_enable_homedirs       off
httpd_execmem               off
httpd_manage_ipa            off
httpd_read_user_content     off
httpd_run_preupgrade        off
httpd_run_stickshift        off
httpd_serve_cobbler_files   off
httpd_setrlimit             off
httpd_ssi_exec              off
httpd_tmp_exec              off
httpd_tty_comm              on
httpd_unified               on
httpd_use_cifs              off
httpd_use_fusefs            off
httpd_use_gpg               off
httpd_use_nfs               off
httpd_use_openstack         off
```

Рис. 7

Многие из переключателей находятся в положении «off».

5. Посмотрим статистику по политике с помощью команды *seinfo*, также определим множество пользователей, ролей и типов. (Рис. 8)

```
Файл  Правка  Вид  Поиск  Терминал  Справка
[root@atoev Guest]# seinfo

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

Classes:          81      Permissions:      237
Sensitivities:    1       Categories:      1024
Types:            3851    Attributes:       291
Users:            9       Roles:           12
Booleans:         228     Cond. Expr.:     268
Allow:            311332  Neverallow:       0
Auditallow:       132     Dontaudit:       260601
Type_trans:       38262   Type_change:      38
Type_member:       48     Role_allow:       19
Role_trans:       368     Range_trans:     5601
Constraints:       90     Validatetrans:    0
Initial SIDs:     27     Fs_use:           23
Genfscon:         83     Portcon:          471
Netifcon:         0      Nodecon:          0
Permissives:      91     Polcap:           2

[root@atoev Guest]#
```

Рис. 8

Пользователей: 9, ролей: 12, типов: 3851.

6. Определим тип файлов и поддиректорий, находящихся в директории `/var/www` с помощью команды `ls -lZ /var/www` (Рис. 9)

```
Файл  Правка  Вид  Поиск  Терминал  Справка
Sensitivities:    1       Categories:      1024
Types:            3851    Attributes:       291
Users:            9       Roles:           12
Booleans:         228     Cond. Expr.:     268
Allow:            311332  Neverallow:       0
Auditallow:       132     Dontaudit:       260601
Type_trans:       38262   Type_change:      38
Type_member:       48     Role_allow:       19
Role_trans:       368     Range_trans:     5601
Constraints:       90     Validatetrans:    0
Initial SIDs:     27     Fs_use:           23
Genfscon:         83     Portcon:          471
Netifcon:         0      Nodecon:          0
Permissives:      91     Polcap:           2

[root@atoev Guest]# 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@atoev Guest]#
```

Рис. 9

7. Определим тип файлов, находящихся в директории `/var/www/html` с помощью команды `ls -lZ /var/www/html` (Рис. 10)

```
Файл  Правка  Вид  Поиск  Терминал  Справка
[Guest@atoev ~]$ su
Пароль:
[root@atoev Guest]# 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@atoev Guest]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.txt
[root@atoev Guest]#
```

Рис. 10

8. Определим круг пользователей, которым разрешено создание файлов в директории */var/www/html*. (Рис. 11)

```
Файл  Правка  Вид  Поиск  Терминал  Справка
[Guest@atoev ~]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[Guest@atoev ~]$ su
Пароль:
[root@atoev Guest]# echo "test" > /var/www/html/test.txt
[root@atoev Guest]# su Guest2
[Guest2@atoev Guest]$ echo "test" > /var/www/html/test1.txt
bash: /var/www/html/test1.txt: Отказано в доступе
[Guest2@atoev Guest]$ su fkatoev
Пароль:
[fkatoev@atoev Guest]$ echo "test" > /var/www/html/test1.txt
bash: /var/www/html/test1.txt: Отказано в доступе
[fkatoev@atoev Guest]$ exit
exit
[Guest2@atoev Guest]$ exit
exit
[root@atoev Guest]#
```

Рис. 11

Видно, что только суперпользователь может создать файл в данной директории.

9. В следствие этого создадим от имени суперпользователя html-файл */var/www/html/test.html* следующего содержания: (Рис. 12)

<html>

<body>test</body>

</html>

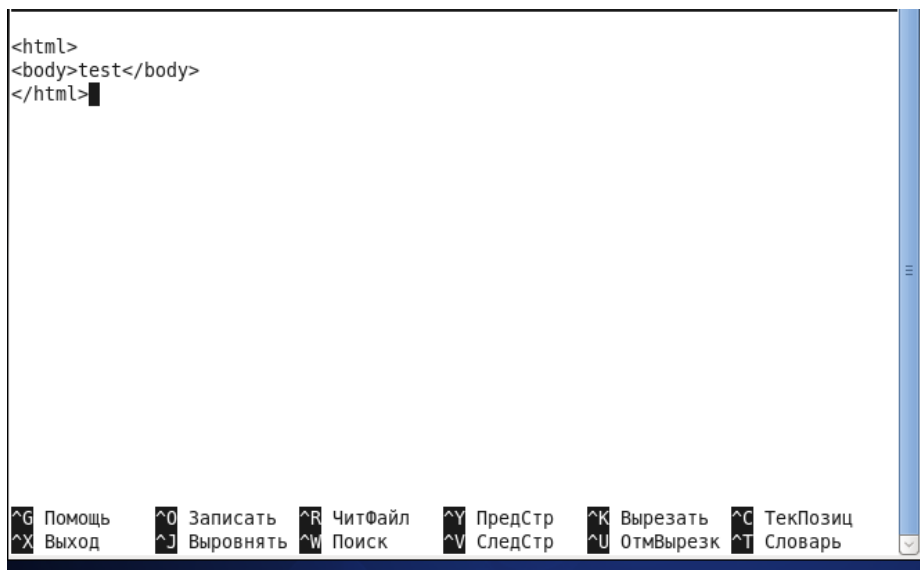


Рис. 12

10. Проверим контекст созданного файла (Рис. 13).

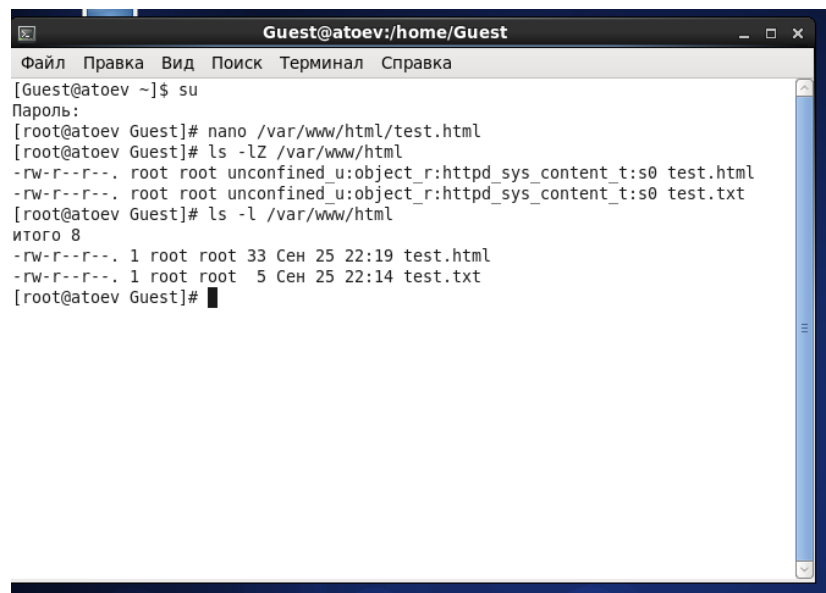


Рис. 13

Контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`: `unconfined_u:object_r:httpd_sys_content_t`

11. Обратимся к файлу через веб-сервер, введя в браузере firefox адрес



<http://127.0.0.1/test.html>

Убедимся, что файл был успешно отображен. (Рис. 14)

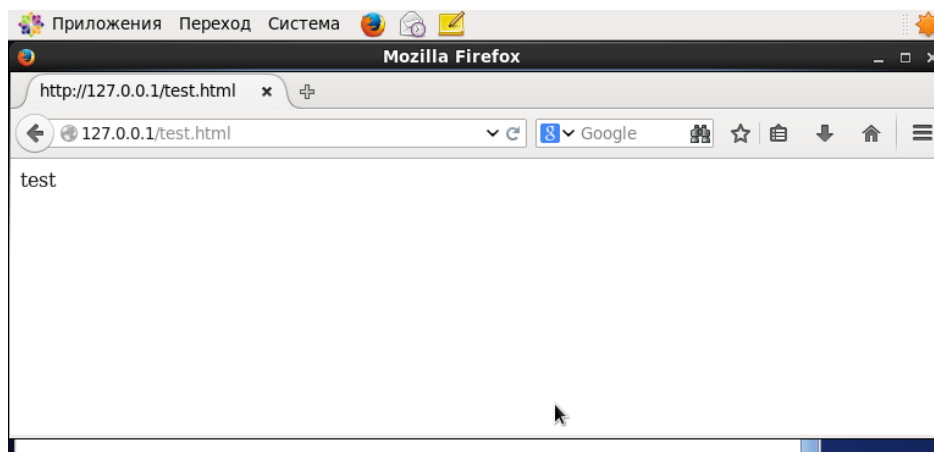


Рис. 14

12. Изучим справку *man httpd\_selinux* и выясним, какие контексты файлов определены для *httpd* и сопоставим их с типом файла *test.html*. Проверим контекст файла командой *ls -Z /var/www/html/test.html* (Рис. 15)



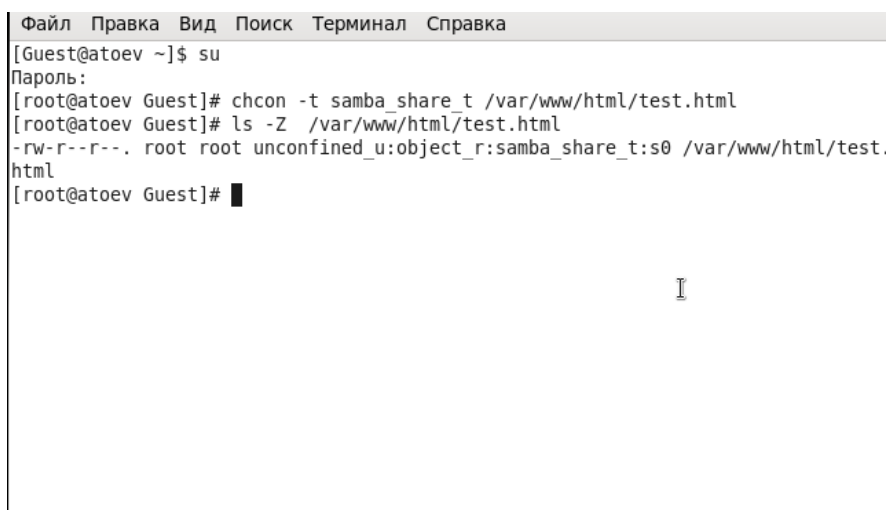
Рис. 15

Т.к. по умолчанию пользователи CentOS являются свободными (unconfined) от типа, 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. Тип *httpd\_sys\_content\_t* позволяет процессу *httpd* получить доступ к файлу. Благодаря наличию последнего типа мы получили доступ к файлу при обращении к нему через браузер.

13. Изменим контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на другой, к которому процесс `httpd` не должен иметь доступа, в нашем случае, на `samba_share_t`: (Рис. 16)

```
chcon -t samba_share_t /var/www/html/test.html
```

```
ls -Z /var/www/html/test.html
```



```
Файл Правка Вид Поиск Терминал Справка
[Guest@atoev ~]$ su
Пароль:
[root@atoev Guest]# chcon -t samba_share_t /var/www/html/test.html
[root@atoev Guest]# 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@atoev Guest]#
```

Рис. 16

Как можно видеть, контекст успешно сменился.

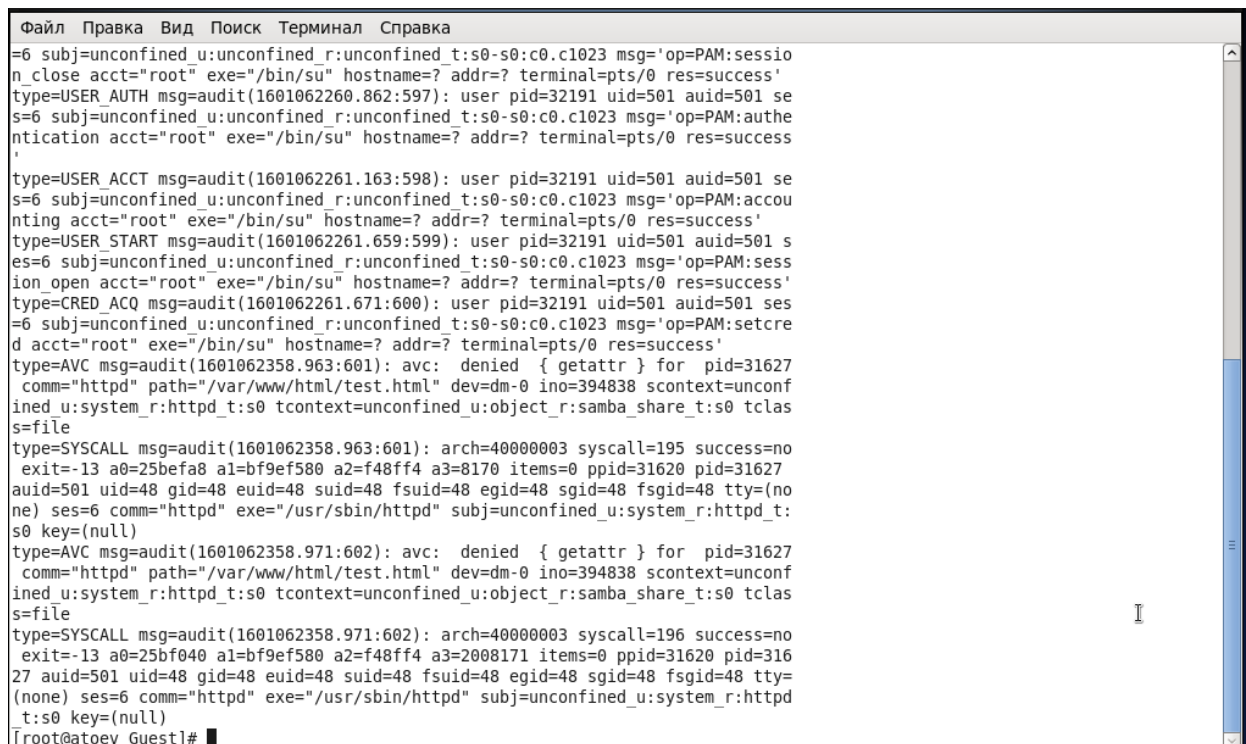
14. Попробуем еще раз получить доступ к файлу через веб-сервер, введя в браузере `firefox` адрес (Рис. 17) <http://127.0.0.1/test.html>



Рис. 17

Мы получили сообщение об ошибке.

15. Проанализируем ситуацию, просмотрев log-файлы веб-сервера Apache, системный log-файл и audit.log при условии уже запущенных процессов setroubleshootd и audtd (Рис. 18)

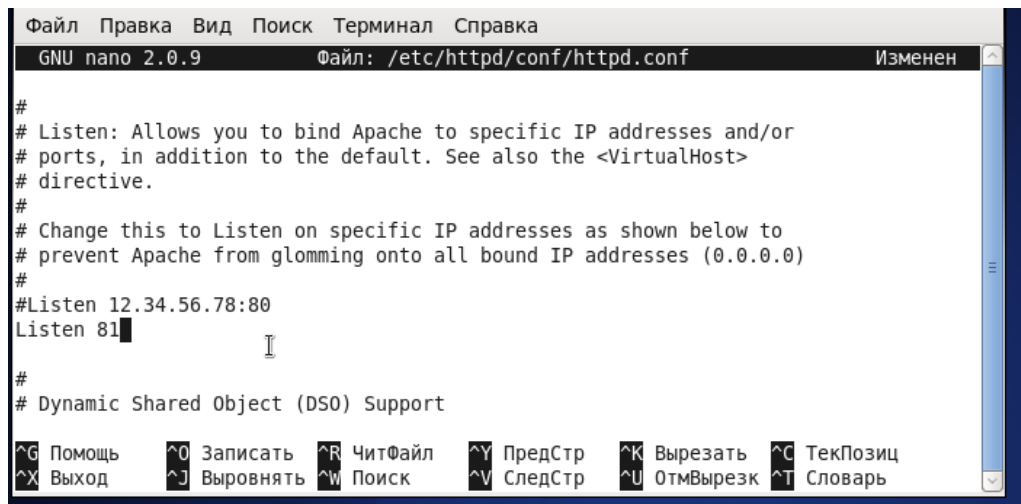


```
Файл Правка Вид Поиск Терминал Справка
=6 subj=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 msg='op=PAM:session_close acct="root" exe="/bin/su" hostname=? addr=? terminal=pts/0 res=success'
type=USER_AUTH msg=audit(1601062260.862:597): user pid=32191 uid=501 auid=501 ses=6 subj=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 msg='op=PAM:authentication acct="root" exe="/bin/su" hostname=? addr=? terminal=pts/0 res=success'
type=USER_ACCT msg=audit(1601062261.163:598): user pid=32191 uid=501 auid=501 ses=6 subj=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 msg='op=PAM:accounting acct="root" exe="/bin/su" hostname=? addr=? terminal=pts/0 res=success'
type=USER_START msg=audit(1601062261.659:599): user pid=32191 uid=501 auid=501 ses=6 subj=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 msg='op=PAM:session_open acct="root" exe="/bin/su" hostname=? addr=? terminal=pts/0 res=success'
type=CRED_ACQ msg=audit(1601062261.671:600): user pid=32191 uid=501 auid=501 ses=6 subj=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 msg='op=PAM:setcred acct="root" exe="/bin/su" hostname=? addr=? terminal=pts/0 res=success'
type=AVC msg=audit(1601062358.963:601): avc: denied { getattr } for pid=31627 comm="httpd" path="/var/www/html/test.html" dev=dm-0 ino=394838 scontext=unconfined u:system_r:httpd_t:s0 tcontext=unconfined u:object_r:samba_share_t:s0 tclass=file
type=SYSCALL msg=audit(1601062358.963:601): arch=40000003 syscall=195 success=no exit=-13 a0=25befa8 a1=bf9ef580 a2=f48ff4 a3=8170 items=0 ppid=31620 pid=31627 auid=501 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=6 comm="httpd" exe="/usr/sbin/httpd" subj=unconfined_u:system_r:httpd_t:s0 key=(null)
type=AVC msg=audit(1601062358.971:602): avc: denied { getattr } for pid=31627 comm="httpd" path="/var/www/html/test.html" dev=dm-0 ino=394838 scontext=unconfined u:system_r:httpd_t:s0 tcontext=unconfined u:object_r:samba_share_t:s0 tclass=file
type=SYSCALL msg=audit(1601062358.971:602): arch=40000003 syscall=196 success=no exit=-13 a0=25bf040 a1=bf9ef580 a2=f48ff4 a3=2008171 items=0 ppid=31620 pid=31627 auid=501 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=6 comm="httpd" exe="/usr/sbin/httpd" subj=unconfined_u:system_r:httpd_t:s0 key=(null)
[root@atoev Guest]#
```

Рис. 18

Исходя из log-файлов, мы можем заметить, что проблема в измененном контексте на шаге 13, т.к. процесс httpd не имеет доступа на samba\_share\_t. В системе оказались запущены процессы setroubleshootd и audtd, поэтому ошибки, связанные с измененным контекстом, также есть в файле */var/log/audit/audit.log*.

16. Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в */etc/services*), заменив в файле */etc/httpd/conf/httpd.conf* строчку *Listen 80* на *Listen 81*.



```
Файл  Правка  Вид  Поиск  Терминал  Справка
GNU nano 2.0.9      Файл: /etc/httpd/conf/httpd.conf      Изменен

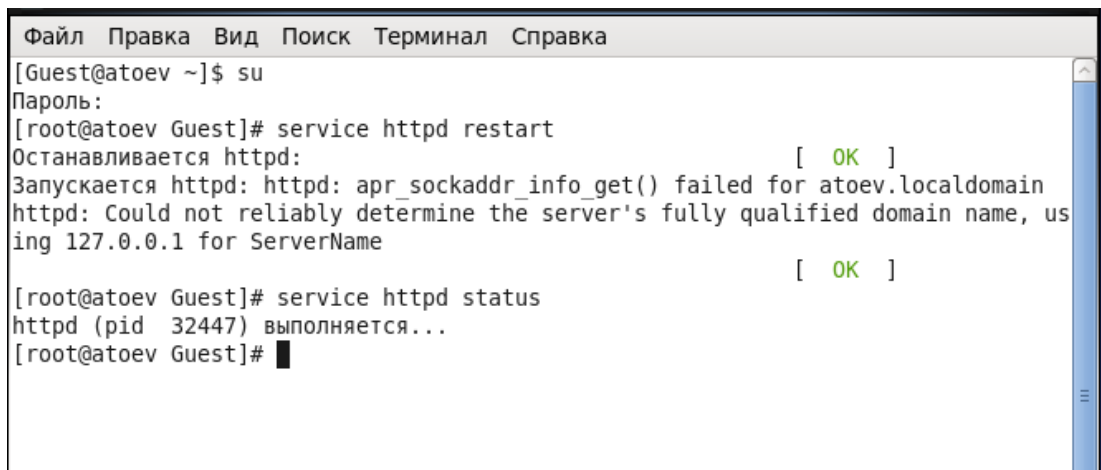
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, in addition to the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses (0.0.0.0)
#
#Listen 12.34.56.78:80
Listen 81

#
# Dynamic Shared Object (DSO) Support

^G  Помощь    ^O  Записать    ^R  ЧитФайл    ^Y  ПредСтр    ^K  Вырезать    ^C  ТекПозиц
^X  Выход      ^J  Вывернуть   ^W  Поиск      ^V  СледСтр    ^U  ОтмВырезк   ^T  Словарь
```

Рис. 19

17. Перезапустим веб-сервер Апасче и попробуем обратиться к файлу через веб-сервер, введя в браузере firefox адрес <http://127.0.0.1/test.html>



```
Файл  Правка  Вид  Поиск  Терминал  Справка
[Guest@atoev ~]$ su
Пароль:
[root@atoev Guest]# service httpd restart
Останавливается httpd: [ OK ]
Запускается httpd: httpd: apr_sockaddr_info_get() failed for atoev.localdomain
httpd: Could not reliably determine the server's fully qualified domain name, us
ing 127.0.0.1 for ServerName [ OK ]

[root@atoev Guest]# service httpd status
httpd (pid 32447) выполняется...
[root@atoev Guest]#
```

Рис. 20

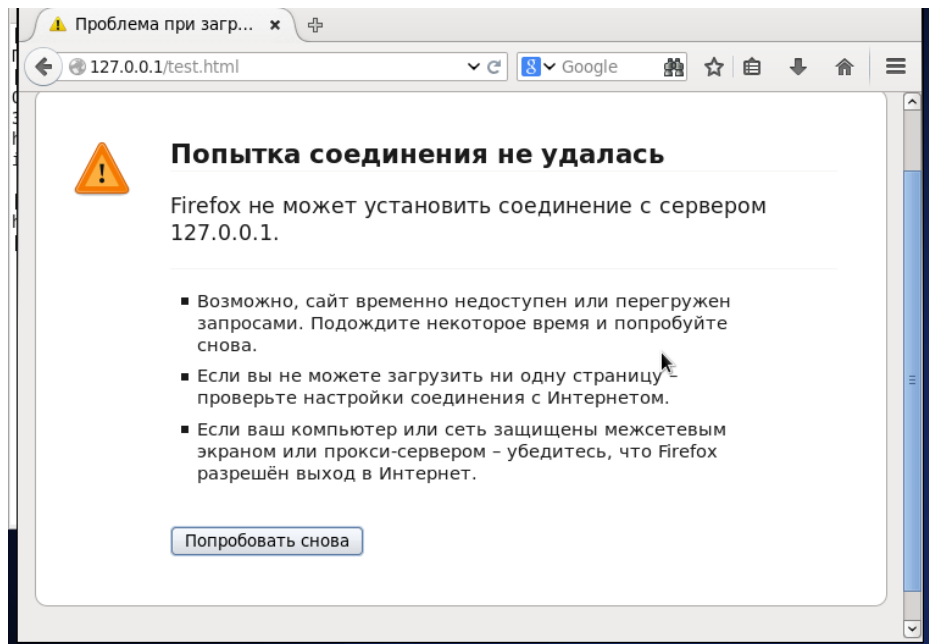


Рис. 21

Из того, что при запуске файла через браузер появилась ошибка, можно сделать предположение, что в списках портов, работающих с веб-сервером Apache, отсутствует порт 81.

18. Подтвердим свои догадки, проанализировав log-файлы: `tail -n1 /var/log/messages` и просмотрев файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log`

```

Приложения  Переход  Система
Guest@atoev:/home/Guest
Файл  Правка  Вид  Поиск  Терминал  Справка
[root@atoev Guest]# tail /var/log/audit/audit.log
type=USER_AUTH msg=audit(1601062938.231:611): user pid=32405 uid=501 auid=50
1 ses=6 subj=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 msg='op=P
AM:authentication acct="root" exe="/bin/su" hostname=? addr=? terminal=pts/0
res=success'
type=USER_ACCT msg=audit(1601062938.548:612): user pid=32405 uid=501 auid=50
1 ses=6 subj=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 msg='op=P
AM:accounting acct="root" exe="/bin/su" hostname=? addr=? terminal=pts/0 res
=success'
type=USER_START msg=audit(1601062939.135:613): user pid=32405 uid=501 auid=5
01 ses=6 subj=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 msg='op=
PAM:session_open acct="root" exe="/bin/su" hostname=? addr=? terminal=pts/0
res=success'
type=CRED_ACQ msg=audit(1601062939.144:614): user pid=32405 uid=501 auid=501
ses=6 subj=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 msg='op=PA
M:setcred acct="root" exe="/bin/su" hostname=? addr=? terminal=pts/0 res=suc
cess'
type=USER_ACCT msg=audit(1601063402.276:615): user pid=32510 uid=0 auid=4294
967295 ses=4294967295 subj=system u:system r:cron t:s0-s0:c0.c1023 msg='op=
PAM:accounting acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=
cron res=success'
type=CRED_ACQ msg=audit(1601063402.280:616): user pid=32510 uid=0 auid=42949
67295 ses=4294967295 subj=system u:system r:cron t:s0-s0:c0.c1023 msg='op=P
AM:setcred acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron
res=success'
type=LOGIN msg=audit(1601063402.289:617): pid=32510 uid=0 subj=system u:syst
em r:cron t:s0-s0:c0.c1023 old auid=4294967295 new auid=0 old ses=429496729
5 new ses=56
type=USER_START msg=audit(1601063402.305:618): user pid=32510 uid=0 auid=0 s
es=56 subj=system u:system r:cron t:s0-s0:c0.c1023 msg='op=PAM:session_open
acct="root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=succes
s'
type=CRED_DISP msg=audit(1601063402.737:619): user pid=32510 uid=0 auid=0 se
s=56 subj=system u:system r:cron t:s0-s0:c0.c1023 msg='op=PAM:setcred acct=
"root" exe="/usr/sbin/crond" hostname=? addr=? terminal=cron res=success'

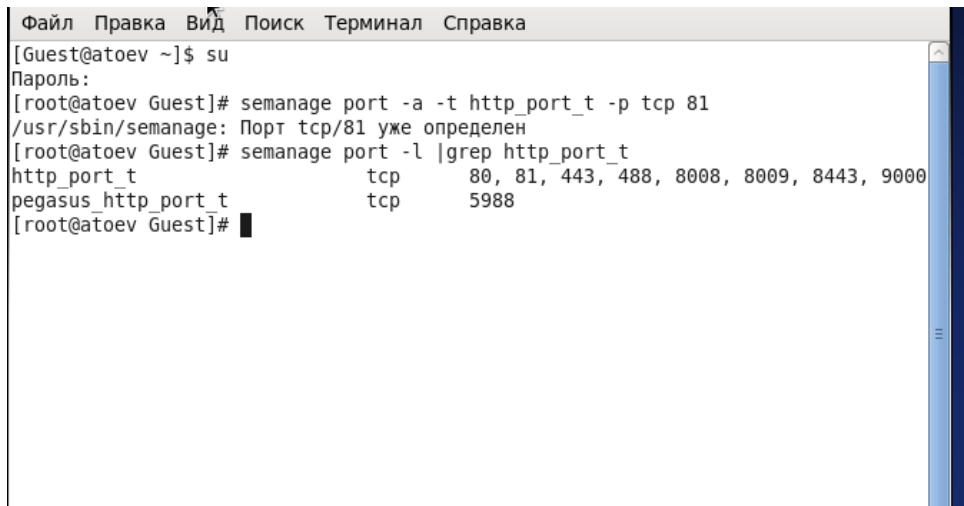
```

Рис. 22

Во всех log-файлах появились записи, кроме `/var/log/messages`.

19. 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`

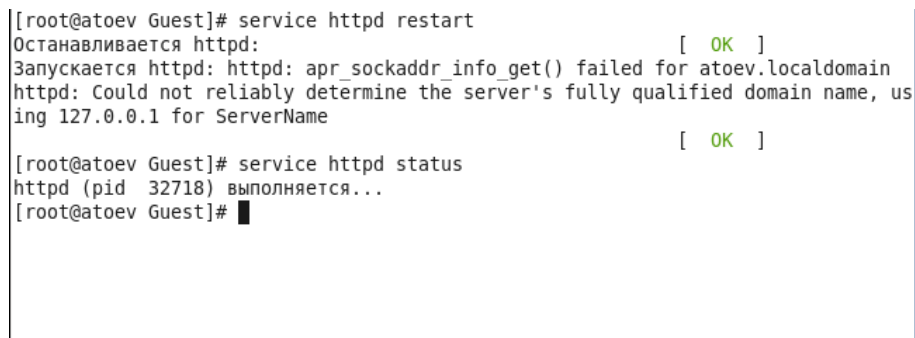


```
Файл Правка Вид Поиск Терминал Справка
[Guest@atoev ~]$ su
Пароль:
[root@atoev Guest]# semanage port -a -t http_port_t -p tcp 81
/usr/sbin/semanage: Порт tcp/81 уже определен
[root@atoev Guest]# semanage port -l |grep http_port_t
http_port_t                tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t        tcp      5988
[root@atoev Guest]#
```

Рис. 23

Убедились, что порт 81 присутствует в списке.

20. Попробуем теперь запустить веб-сервер Apache еще раз.



```
[root@atoev Guest]# service httpd restart
Останавливается httpd: [ OK ]
Запускается httpd: httpd: apr_sockaddr_info_get() failed for atoev.localdomain
httpd: Could not reliably determine the server's fully qualified domain name, us
ing 127.0.0.1 for ServerName [ OK ]
[root@atoev Guest]# service httpd status
httpd (pid 32718) выполняется...
[root@atoev Guest]#
```

Рис. 24

21. Вернем контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`:

**`chcon -t httpd_sys_content_t /var/www/html/test.html`**

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

Рис. 25

После этого вновь попробуем получить доступ к файлу через веб-сервер, введя в браузере firefox адрес <http://127.0.0.1:81/test.html>

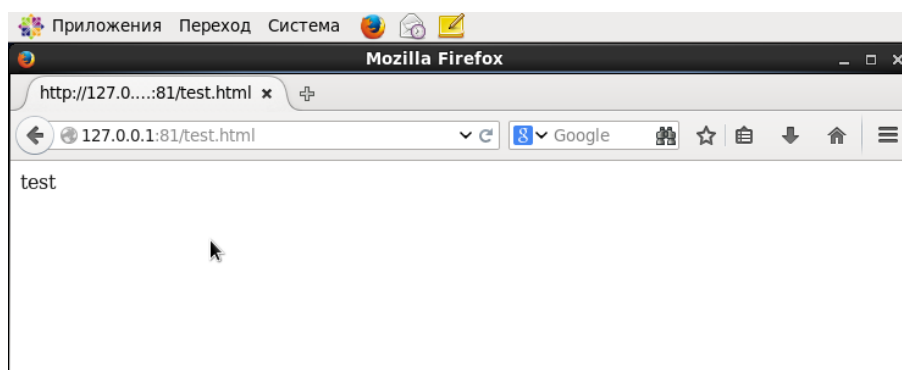


Рис. 26

Увидели слово содержимое файла - слово «test».

22. Исправим обратно конфигурационный файл apache, вернув Listen 80.

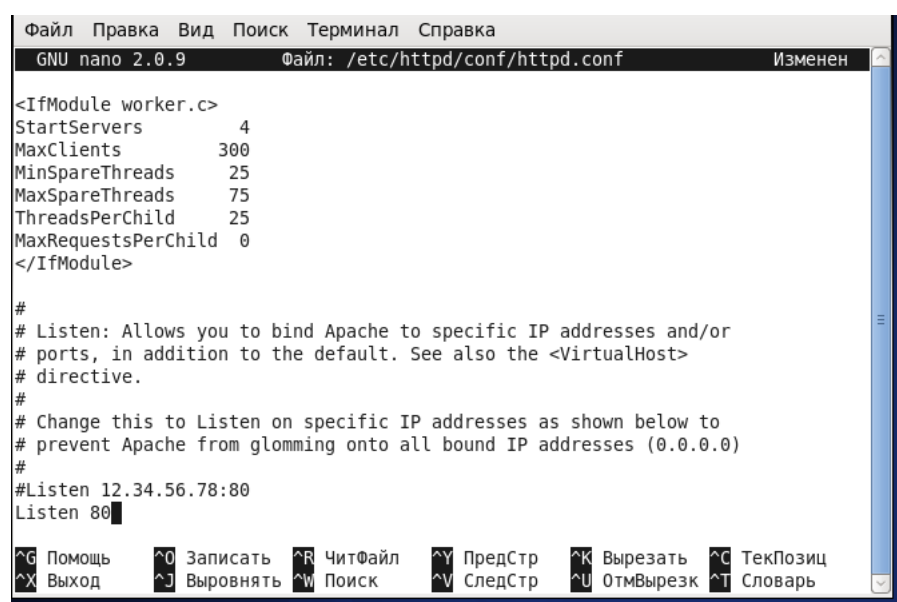
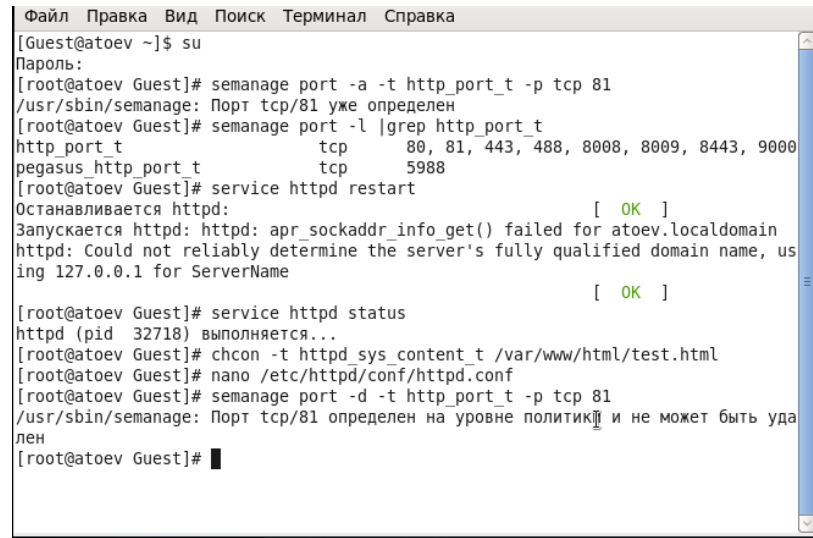


Рис. 27

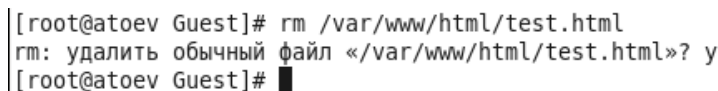
23. Удалим привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81`. Данную команду выполнить невозможно на моей версии CentOS, поэтому получаем ошибку.



```
Файл  Правка  Вид  Поиск  Терминал  Справка
[Guest@atoev ~]$ su
Пароль:
[root@atoev Guest]# semanage port -a -t http_port_t -p tcp 81
/usr/sbin/semanage: Порт tcp/81 уже определен
[root@atoev Guest]# 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@atoev Guest]# service httpd restart
Останавливается httpd: [ OK ]
Запускается httpd: httpd: apr_sockaddr_info_get() failed for atoev.localdomain
httpd: Could not reliably determine the server's fully qualified domain name, us
ing 127.0.0.1 for ServerName [ OK ]
[root@atoev Guest]# service httpd status
httpd (pid 32718) выполняется...
[root@atoev Guest]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@atoev Guest]# nano /etc/httpd/conf/httpd.conf
[root@atoev Guest]# semanage port -d -t http_port_t -p tcp 81
/usr/sbin/semanage: Порт tcp/81 определен на уровне политики и не может быть уда
лен
[root@atoev Guest]#
```

Рис. 28

24. Удалим файл `/var/www/html/test.html`: `rm /var/www/html/test.html`



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

Рис. 29

## Вывод

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.