Лабораторная работа №6

Nikita A. Toponen

RUDN University, 9 October 2022 Moscow, Russia

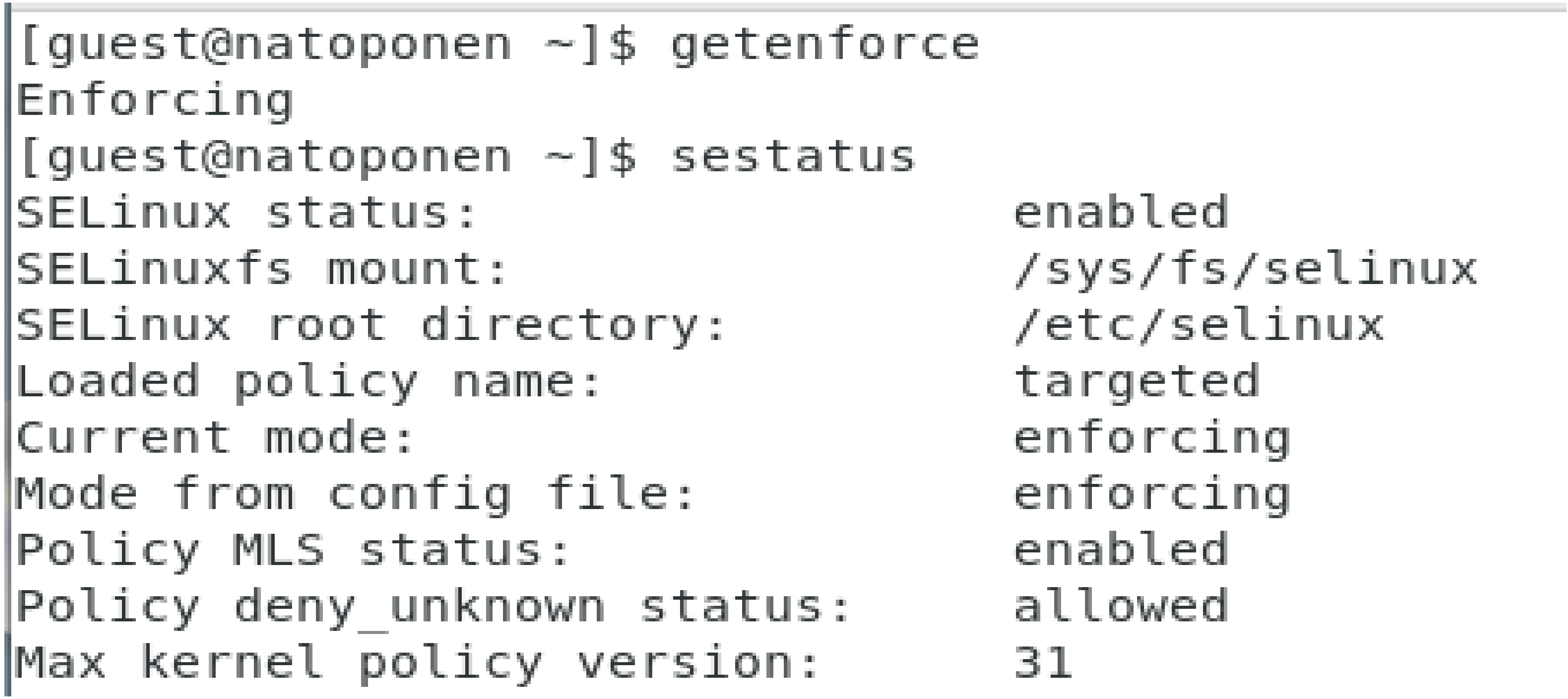
Мандатное разграничение прав в Linux

Цель выполнения работы

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

Выполнение работы

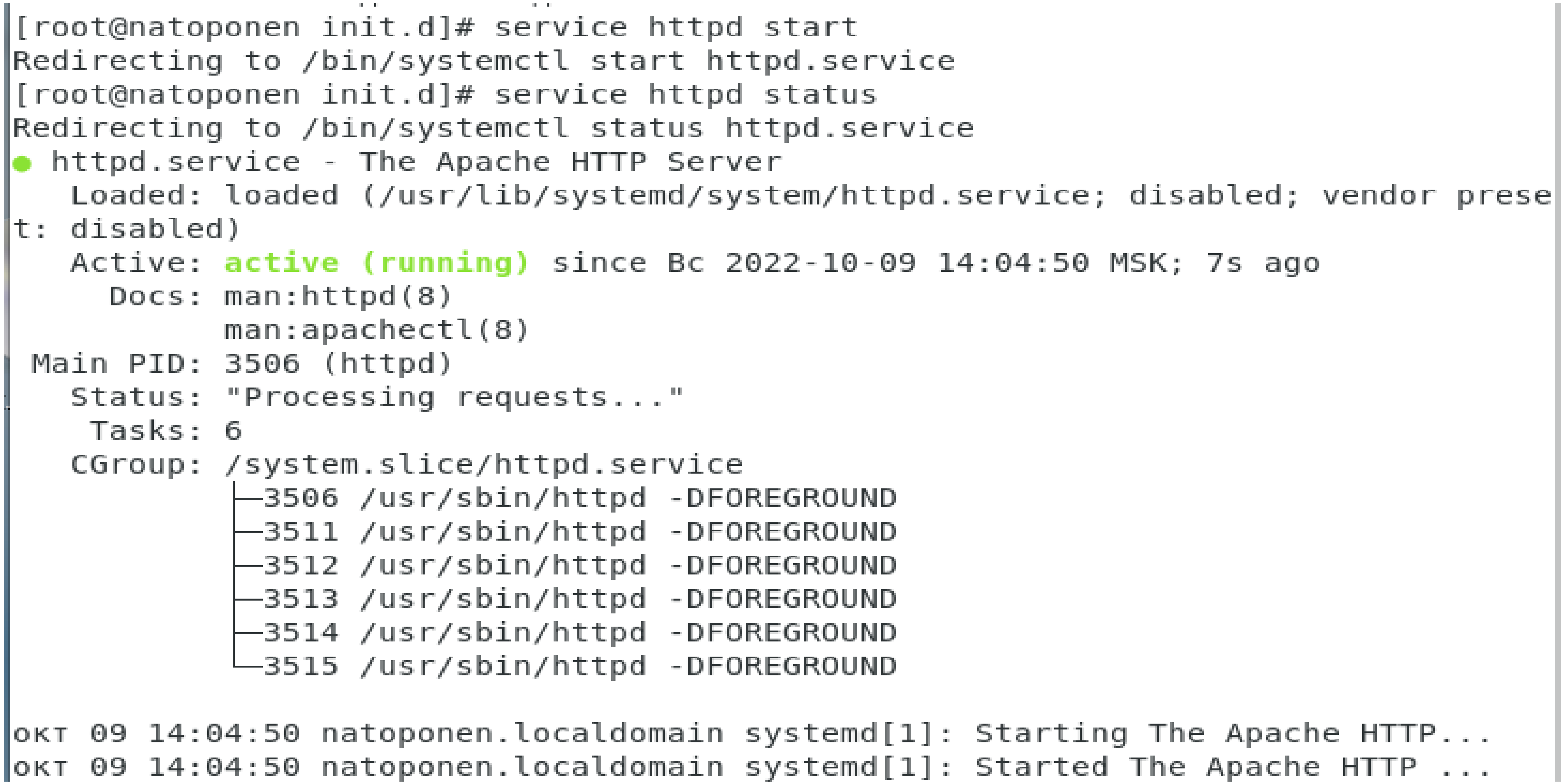
Выполнение работы



```
[guest@natoponen ~]$ getenforce
Enforcing
[guest@natoponen ~]$ 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
```

Рис.1 Режим и политика SELinux

Выполнение работы

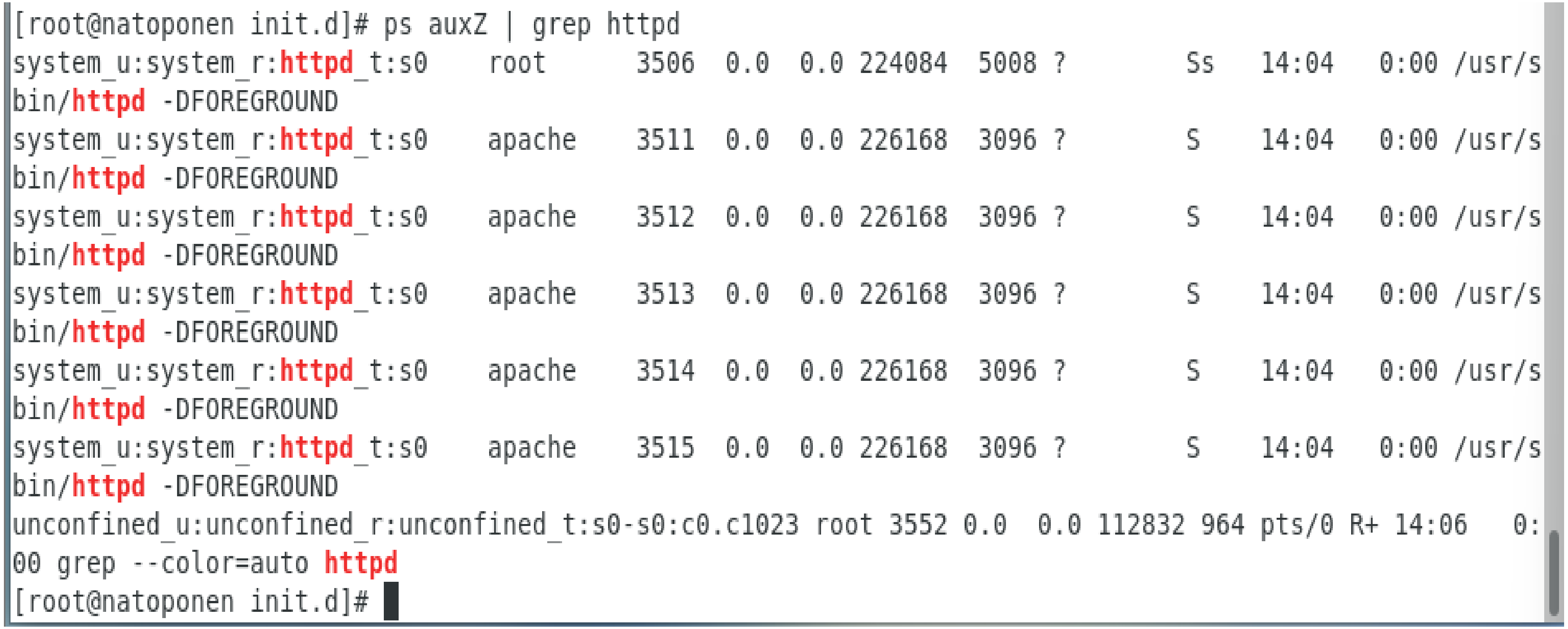


```
[root@natoponen init.d]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@natoponen init.d]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor prese
t: disabled)
   Active: active (running) since Вс 2022-10-09 14:04:50 MSK; 7s ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 3506 (httpd)
   Status: "Processing requests..."
    Tasks: 6
   CGroup: /system.slice/httpd.service
           ├─3506 /usr/sbin/httpd -DFOREGROUND
           ├─3511 /usr/sbin/httpd -DFOREGROUND
           ├─3512 /usr/sbin/httpd -DFOREGROUND
           ├─3513 /usr/sbin/httpd -DFOREGROUND
           ├─3514 /usr/sbin/httpd -DFOREGROUND
           └─3515 /usr/sbin/httpd -DFOREGROUND

окт 09 14:04:50 natoponen.localdomain systemd[1]: Starting The Apache HTTP...
окт 09 14:04:50 natoponen.localdomain systemd[1]: Started The Apache HTTP ...
```

Рис.2 Запуск Apache web server

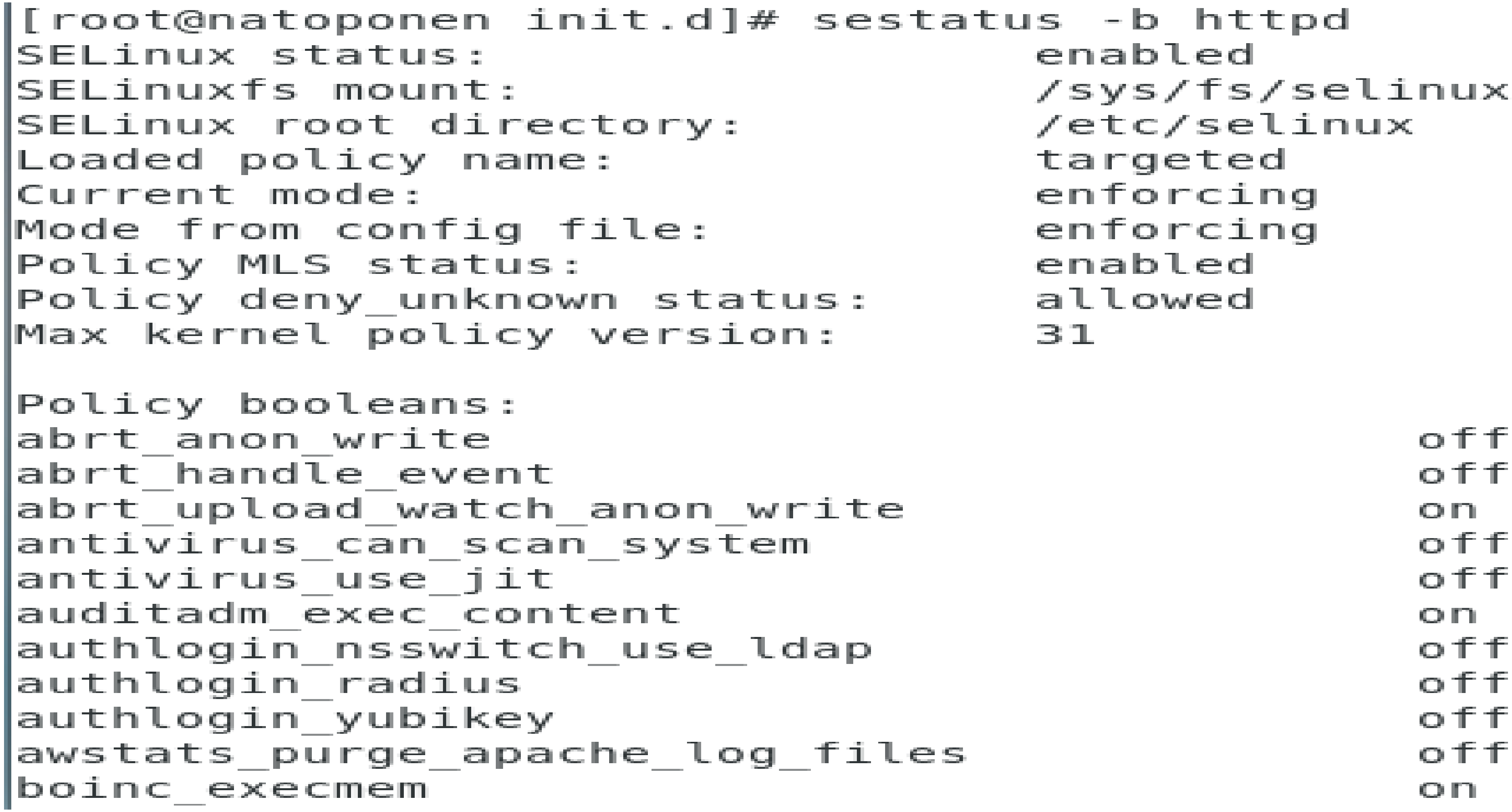
Выполнение работы



```
[root@natoponen init.d]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root      3506  0.0  0.0 224084  5008 ?        Ss   14:04   0:00 /usr/s
bin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3511  0.0  0.0 226168  3096 ?        S    14:04   0:00 /usr/s
bin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3512  0.0  0.0 226168  3096 ?        S    14:04   0:00 /usr/s
bin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3513  0.0  0.0 226168  3096 ?        S    14:04   0:00 /usr/s
bin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3514  0.0  0.0 226168  3096 ?        S    14:04   0:00 /usr/s
bin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3515  0.0  0.0 226168  3096 ?        S    14:04   0:00 /usr/s
bin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3552 0.0  0.0 112832 964 pts/0 R+ 14:06   0:
00 grep --color=auto httpd
[root@natoponen init.d]# 
```

Рис.3 Контекст безопасности Apache web server

Выполнение работы

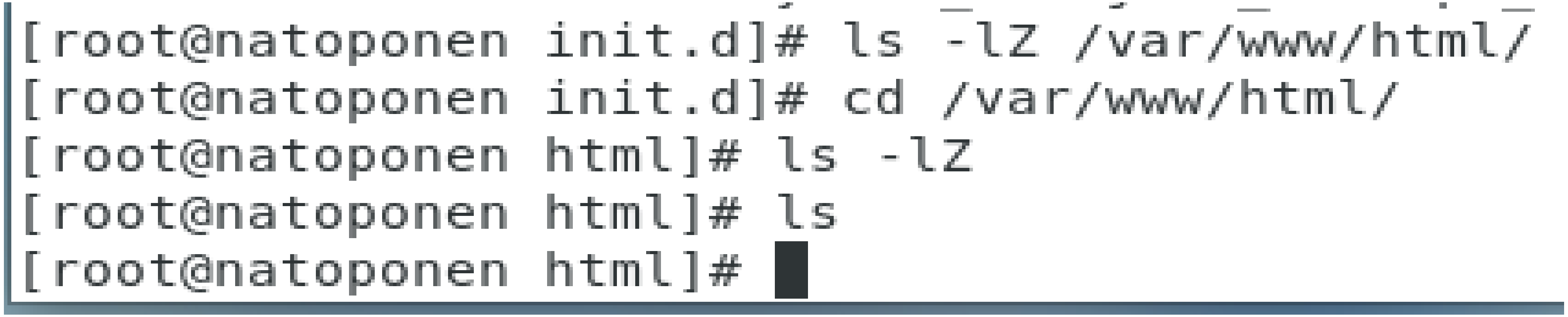


```
[root@natoponen init.d]# sestatus -b httpd
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
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
```

Рис.4 Текущее состояние переключателей SELinux для Apache

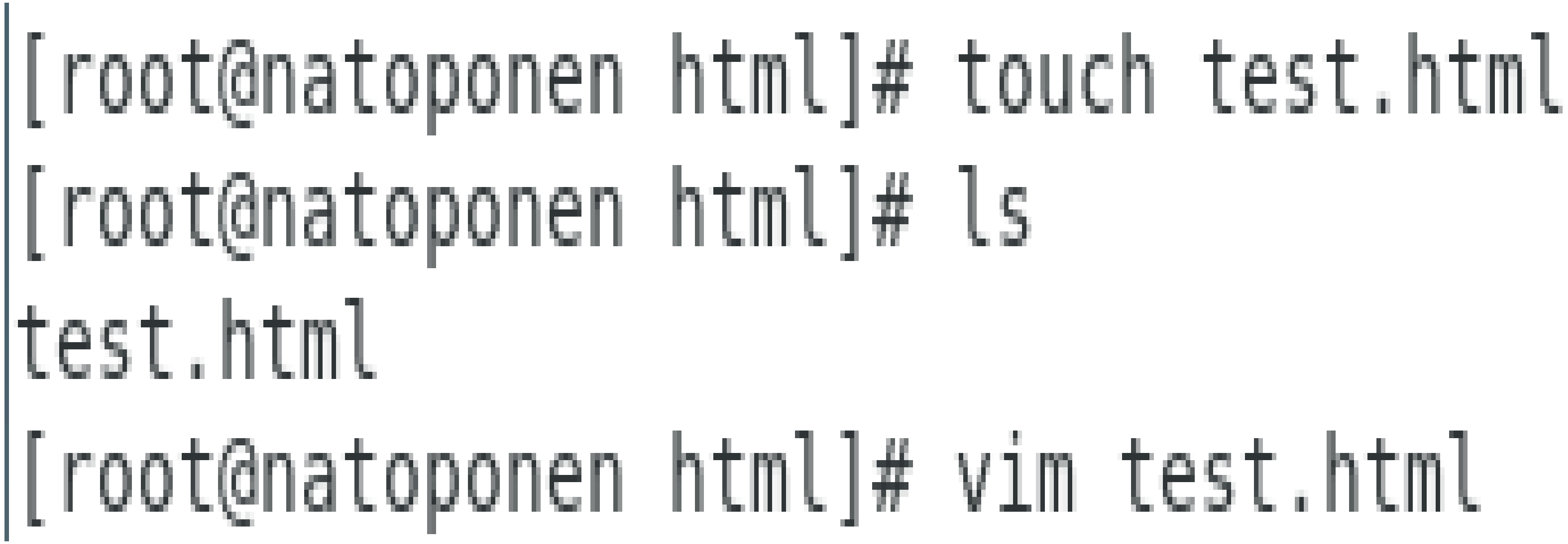
Выполнение работы



```
[root@natoponen init.d]# ls -lZ /var/www/html/
[root@natoponen init.d]# cd /var/www/html/
[root@natoponen html]# ls -lZ
[root@natoponen html]# ls
[root@natoponen html]# █
```

Рис.5 Тип файлов и поддиректорий

Выполнение работы



```
[root@natoponen html]# touch test.html
[root@natoponen html]# ls
test.html
[root@natoponen html]# vim test.html
```

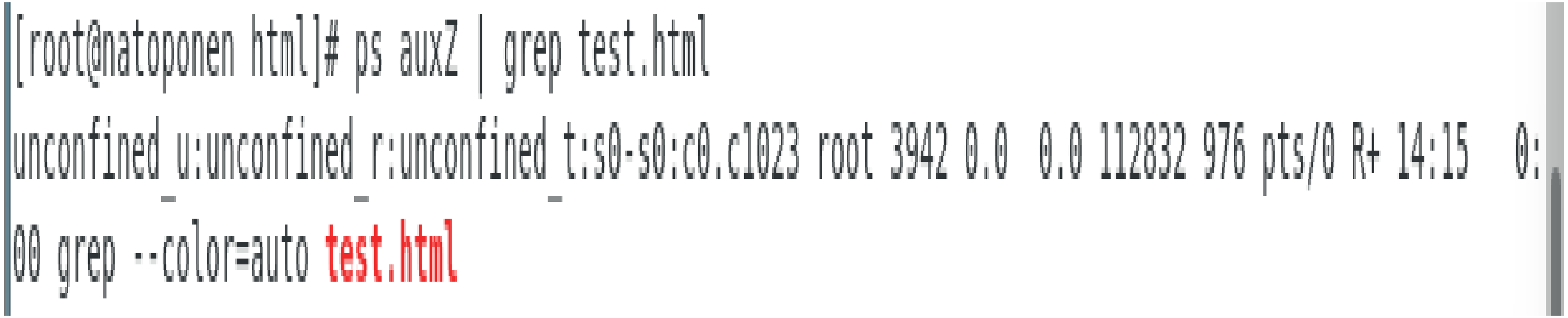
Рис.6 Создание файла test.html

Выполнение работы

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

Текст файла test.html

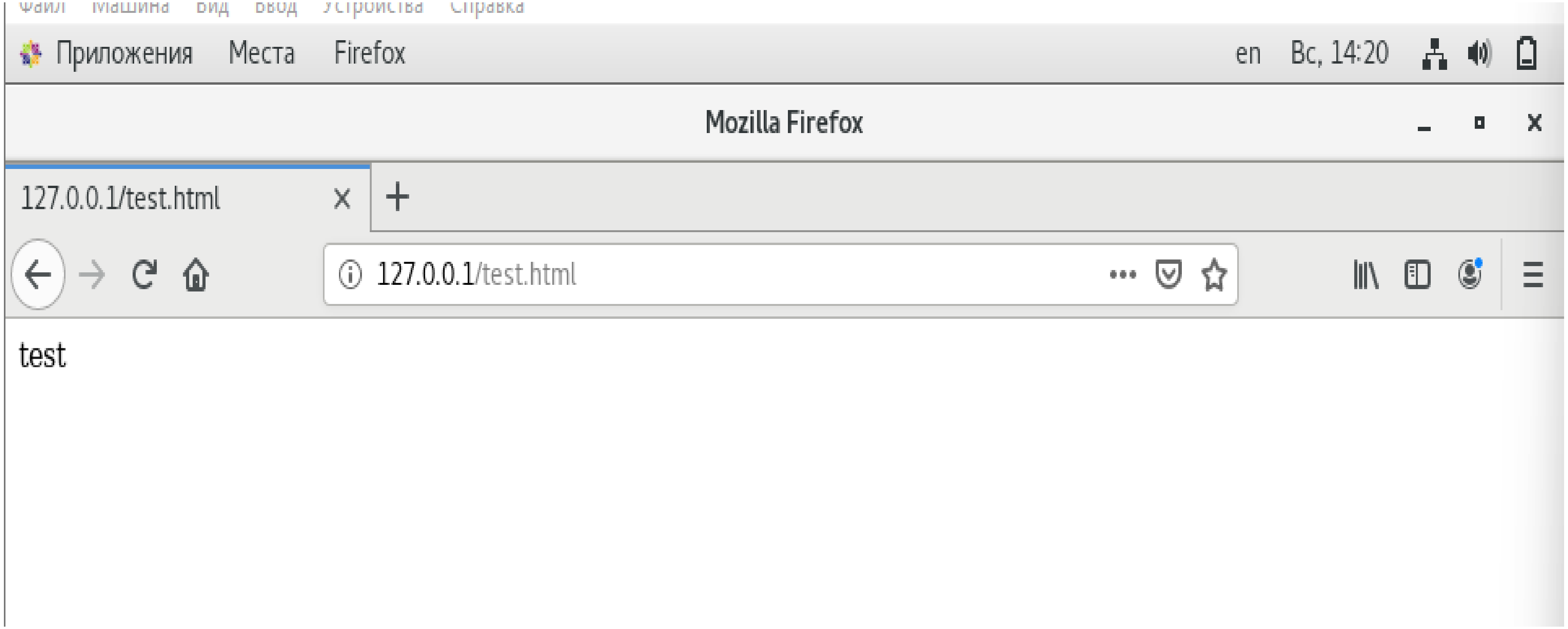
Выполнение работы



```
[root@natoponen html]# ps auxZ | grep test.html
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3942 0.0  0.0 112832 976 pts/0 R+ 14:15   0:
00 grep --color=auto test.html
```

Рис.7 Контекст файла test.html

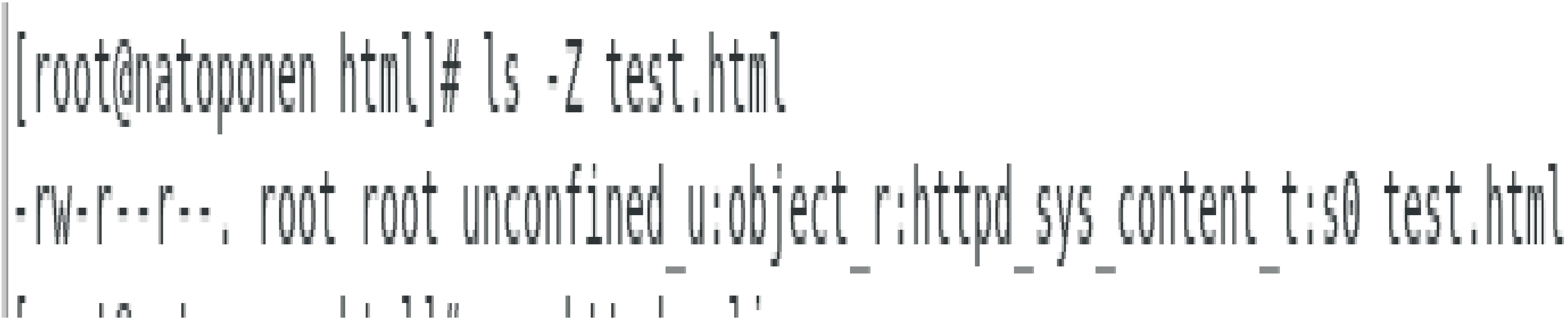
Выполнение работы



test

Рис.8 Веб страница

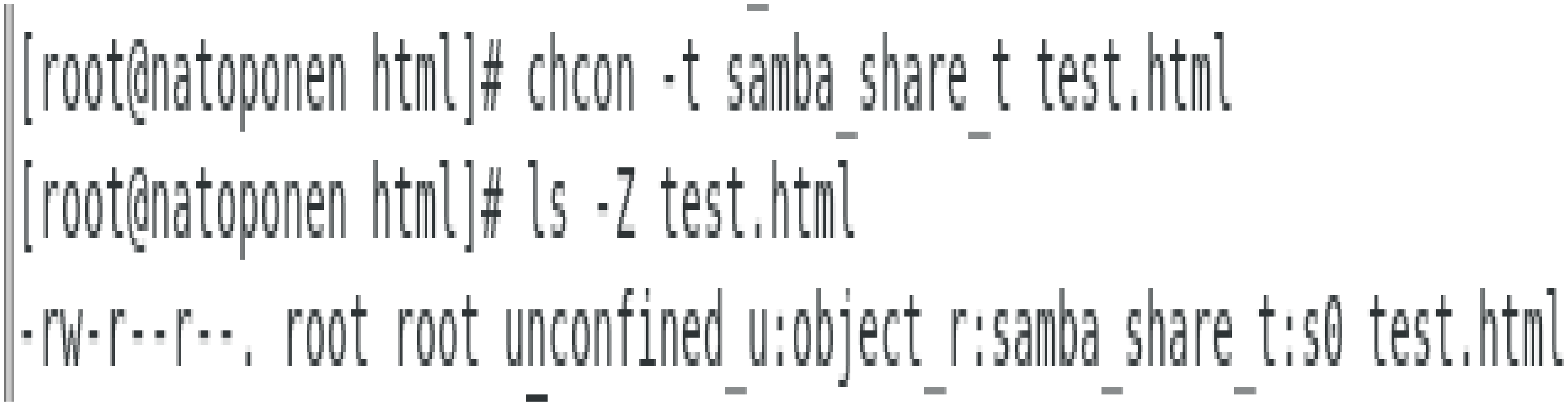
Выполнение работы



```
[root@natoponen html]# ls -Z test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
```

Рис.9 Контекст файла test.html

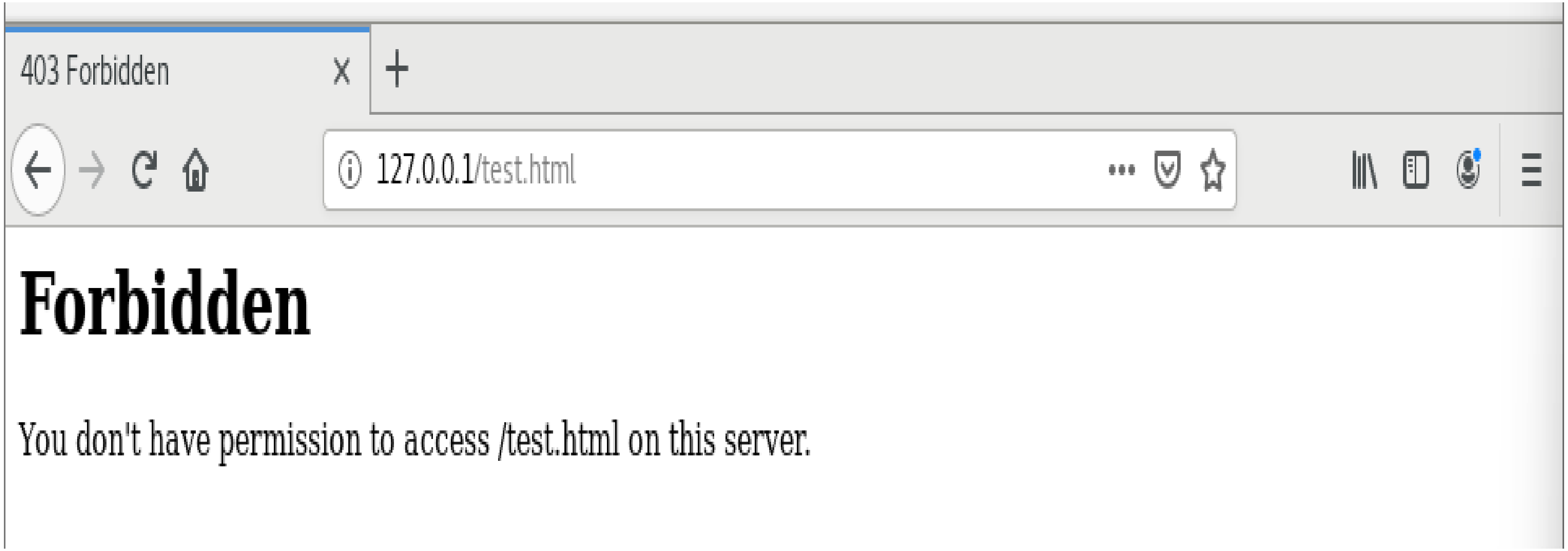
Выполнение работы



```
[root@natoponen html]# chcon -t samba_share_t test.html
[root@natoponen html]# ls -Z test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 test.html
```

Рис.10 Изменения контекста файла test.html

Выполнение работы

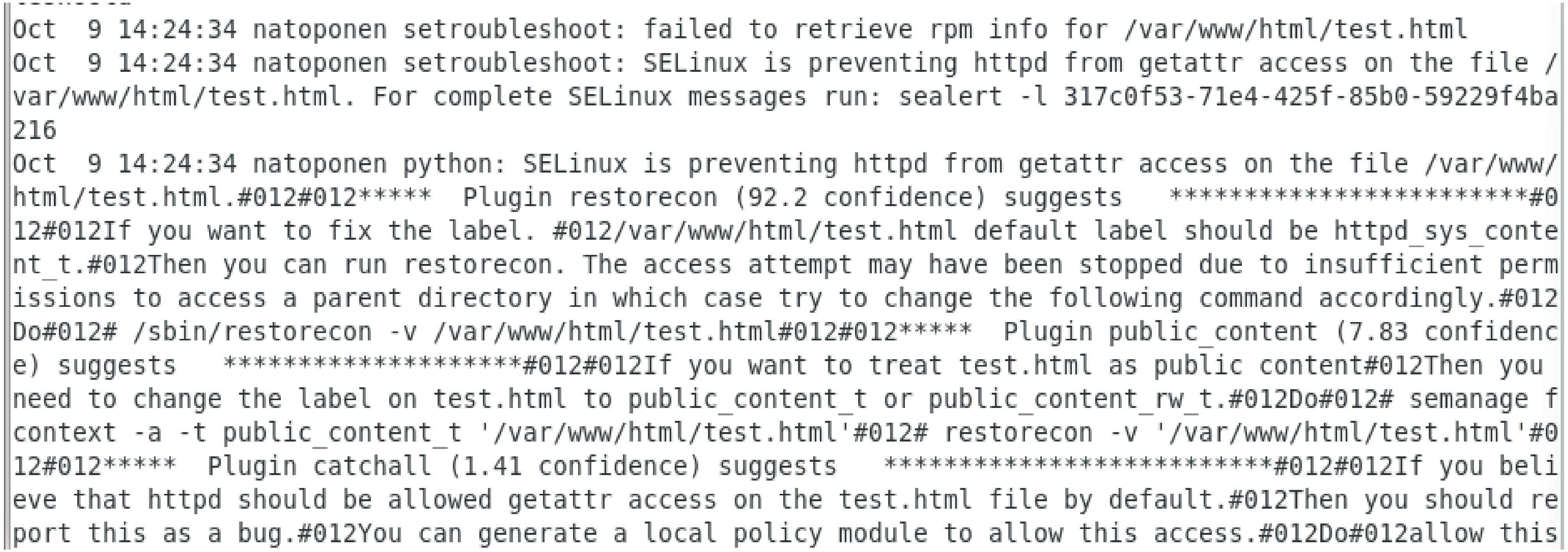


Forbidden

You don't have permission to access /test.html on this server.

Рис.11 Доступ к странице запрещен

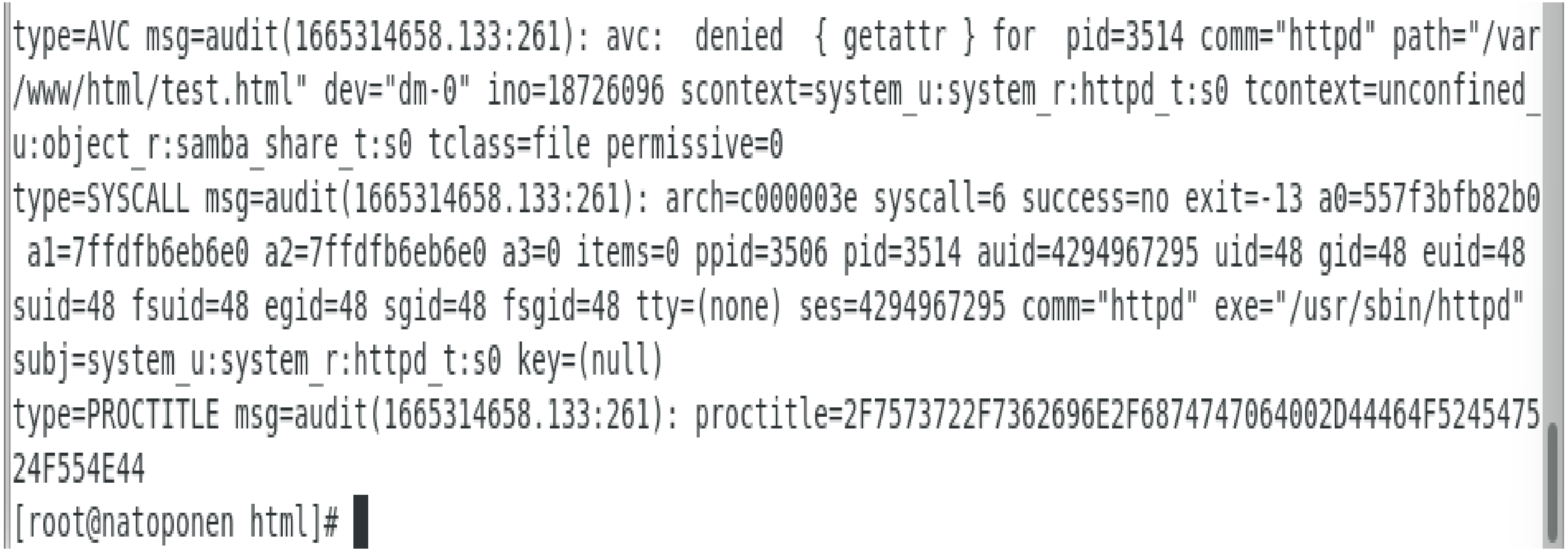
Выполнение работы



```
Oct  9 14:24:34 natoponen setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct  9 14:24:34 natoponen setroubleshoot: SELinux is preventing httpd from getattr access on the file /
var/www/html/test.html. For complete SELinux messages run: sealert -l 317c0f53-71e4-425f-85b0-59229f4ba
216
Oct  9 14:24:34 natoponen python: SELinux is preventing httpd from getattr access on the file /var/www/
html/test.html.#012#012*****  Plugin restorecon (92.2 confidence) suggests   ************************#0
12#012If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_conte
nt_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient perm
issions to access a parent directory in which case try to change the following command accordingly.#012
Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012*****  Plugin public_content (7.83 confidenc
e) suggests   ********************#012#012If you 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 f
context -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#0
12#012*****  Plugin catchall (1.41 confidence) suggests   **************************#012#012If you beli
eve that httpd should be allowed getattr access on the test.html file by default.#012Then you should re
port this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this
```

Рис.12 Логи веб сервера

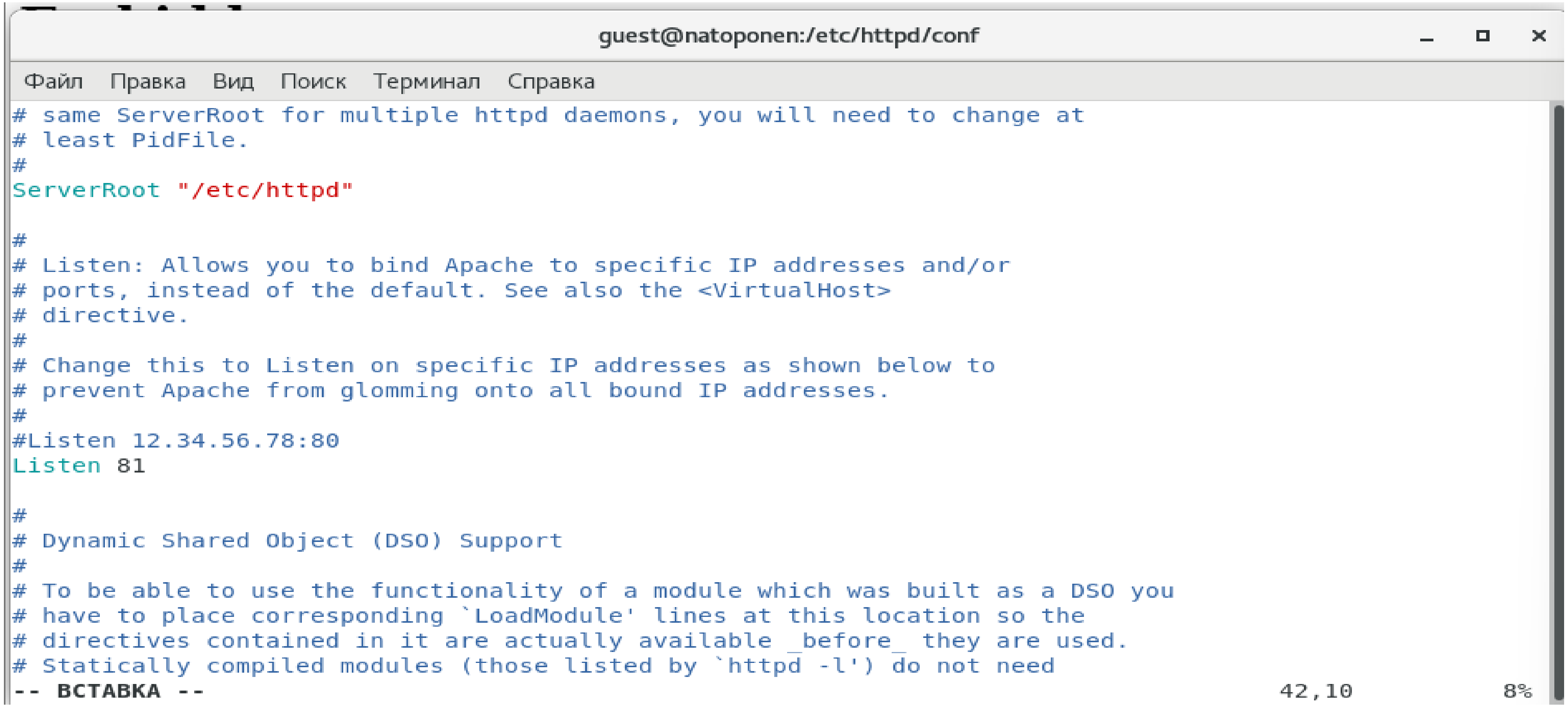
Выполнение работы



```
type=AVC msg=audit(1665314658.133:261): avc:  denied  { getattr } for  pid=3514 comm="httpd" path="/var
/www/html/test.html" dev="dm-0" ino=18726096 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_
u:object_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1665314658.133:261): arch=c000003e syscall=6 success=no exit=-13 a0=557f3bfb82b0
 a1=7ffdfb6eb6e0 a2=7ffdfb6eb6e0 a3=0 items=0 ppid=3506 pid=3514 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(1665314658.133:261): proctitle=2F7573722F7362696E2F6874747064002D44464F5245475
24F554E44
[root@natoponen html]# 
```

Рис.13 Audit логи

Выполнение работы



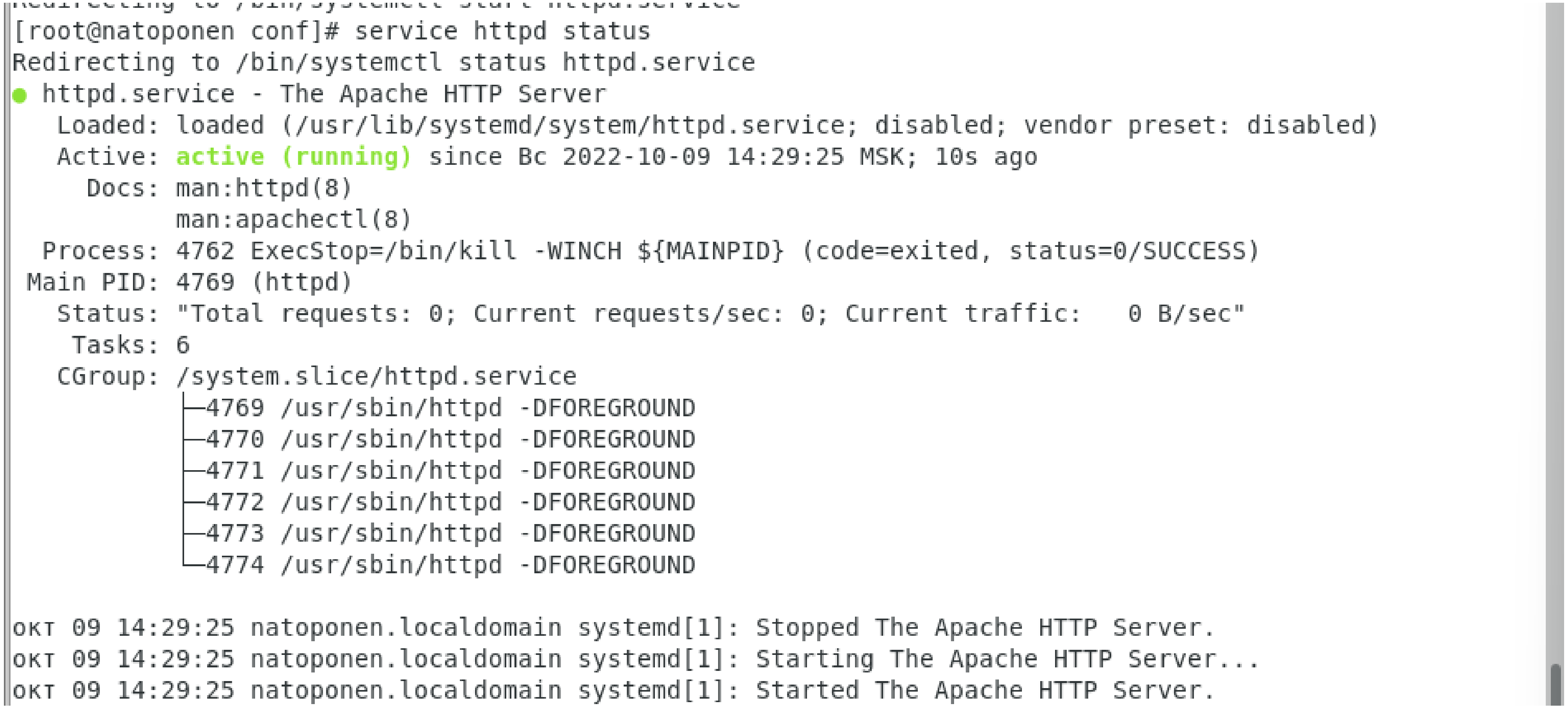
```
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of 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.
#
#Listen 12.34.56.78:80
Listen 81

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding `LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by `httpd -l') do not need
-- ВСТАВКА --                                                        42,10         8%
```

Рис.14 Смена порта

Выполнение работы

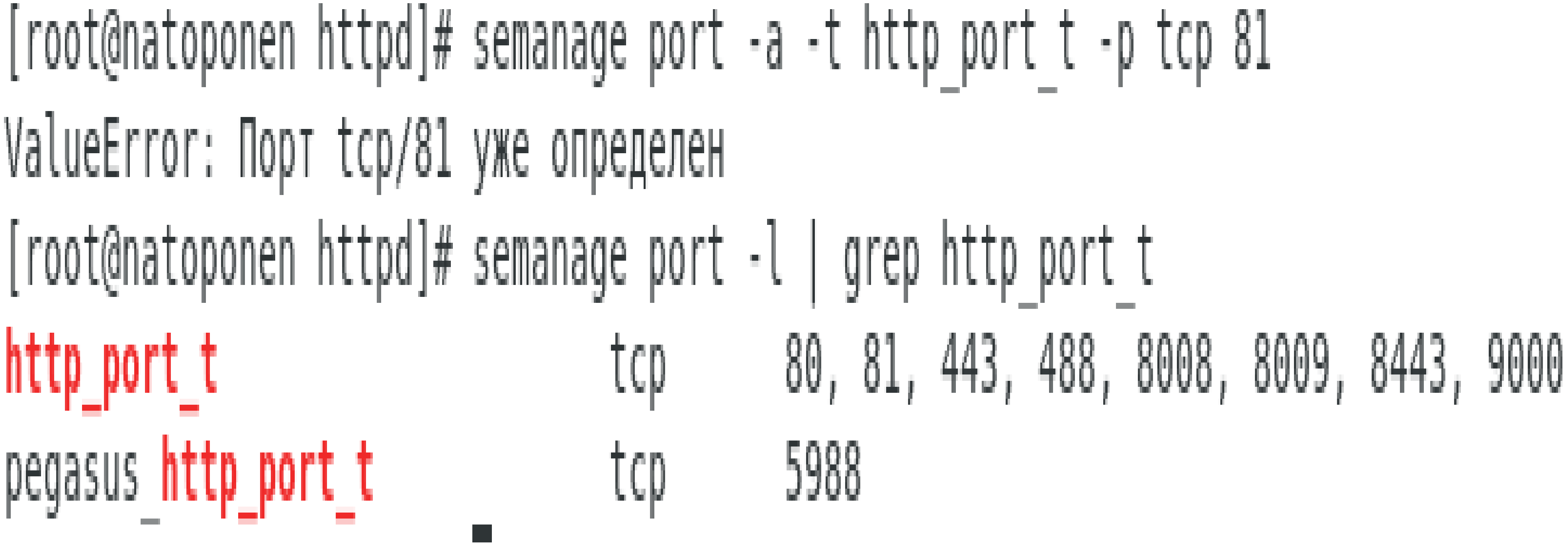


```
Redirecting to /bin/systemctl start httpd.service
[root@natoponen conf]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Вс 2022-10-09 14:29:25 MSK; 10s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 4762 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
 Main PID: 4769 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/sec"
    Tasks: 6
   CGroup: /system.slice/httpd.service
           ├─4769 /usr/sbin/httpd -DFOREGROUND
           ├─4770 /usr/sbin/httpd -DFOREGROUND
           ├─4771 /usr/sbin/httpd -DFOREGROUND
           ├─4772 /usr/sbin/httpd -DFOREGROUND
           ├─4773 /usr/sbin/httpd -DFOREGROUND
           └─4774 /usr/sbin/httpd -DFOREGROUND

окт 09 14:29:25 natoponen.localdomain systemd[1]: Stopped The Apache HTTP Server.
окт 09 14:29:25 natoponen.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 09 14:29:25 natoponen.localdomain systemd[1]: Started The Apache HTTP Server.
```

Рис.15 Запуск на 81 порту

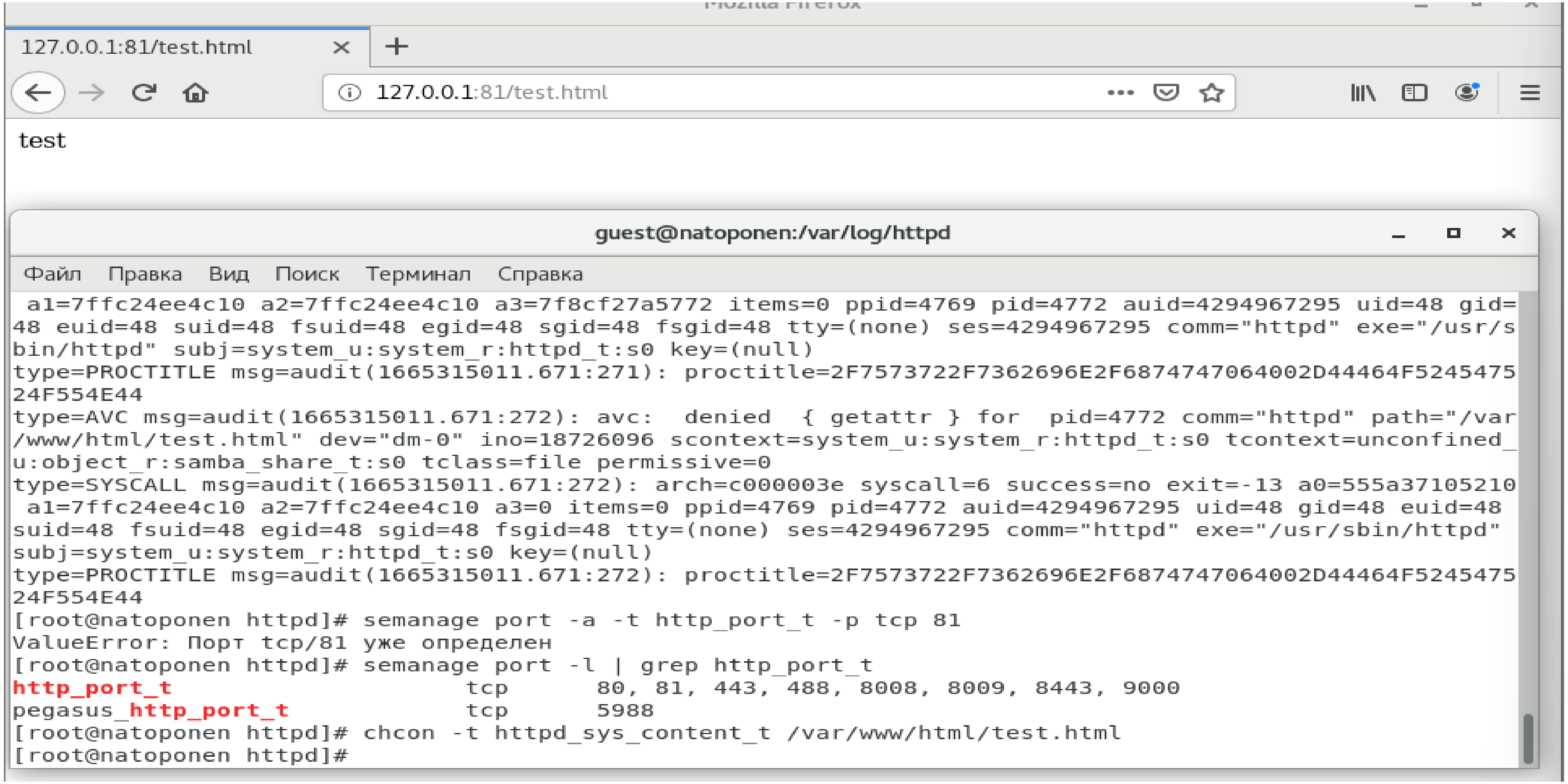
Выполнение работы



```
[root@natoponen httpd]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@natoponen 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.16 Установление порта

Выполнение работы

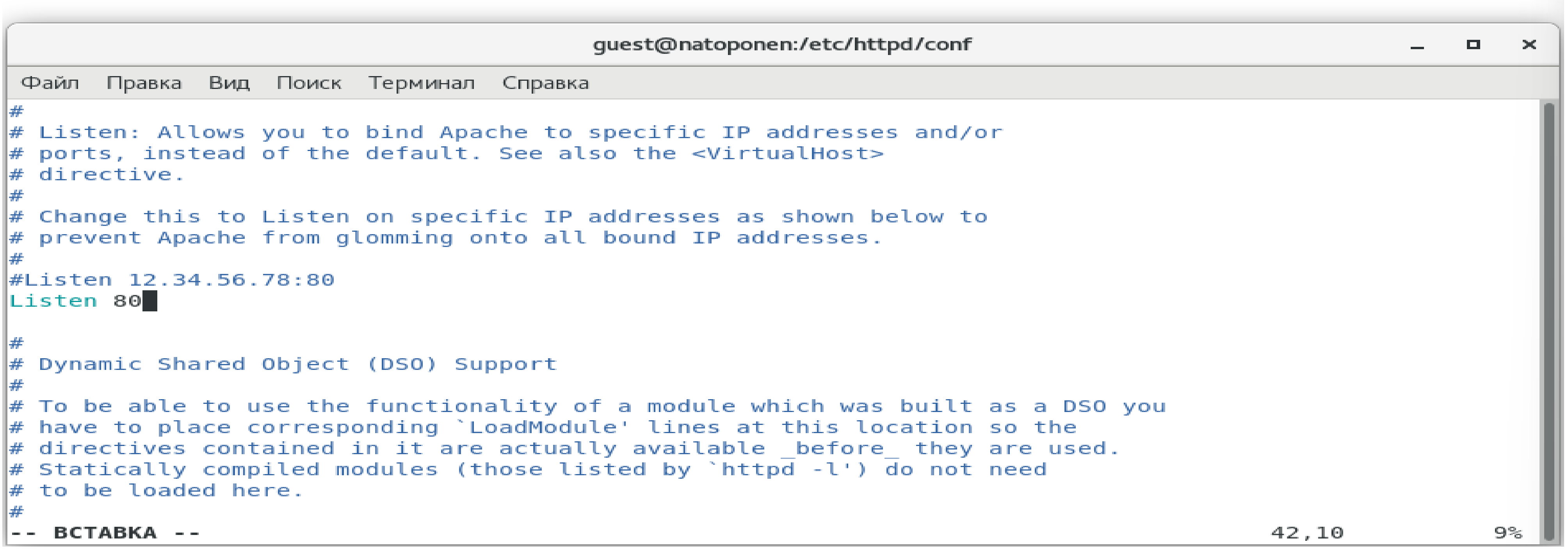

Mozilla Firefox
127.0.0.1:81/test.html
127.0.0.1:81/test.html
guest@natoponen:/var/log/httpd
Файл Правка Вид Поиск Терминал Справка

test

```
 a1=7ffc24ee4c10 a2=7ffc24ee4c10 a3=7f8cf27a5772 items=0 ppid=4769 pid=4772 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/s
bin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)
type=PROCTITLE msg=audit(1665315011.671:271): proctitle=2F7573722F7362696E2F6874747064002D44464F5245475
24F554E44
type=AVC msg=audit(1665315011.671:272): avc:  denied  { getattr } for  pid=4772 comm="httpd" path="/var
/www/html/test.html" dev="dm-0" ino=18726096 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_
u:object_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1665315011.671:272): arch=c000003e syscall=6 success=no exit=-13 a0=555a37105210
 a1=7ffc24ee4c10 a2=7ffc24ee4c10 a3=0 items=0 ppid=4769 pid=4772 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(1665315011.671:272): proctitle=2F7573722F7362696E2F6874747064002D44464F5245475
24F554E44
[root@natoponen httpd]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@natoponen 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
[root@natoponen httpd]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@natoponen httpd]#
```

Рис.17 Работа веб сервера на 81 порту

Выполнение работы



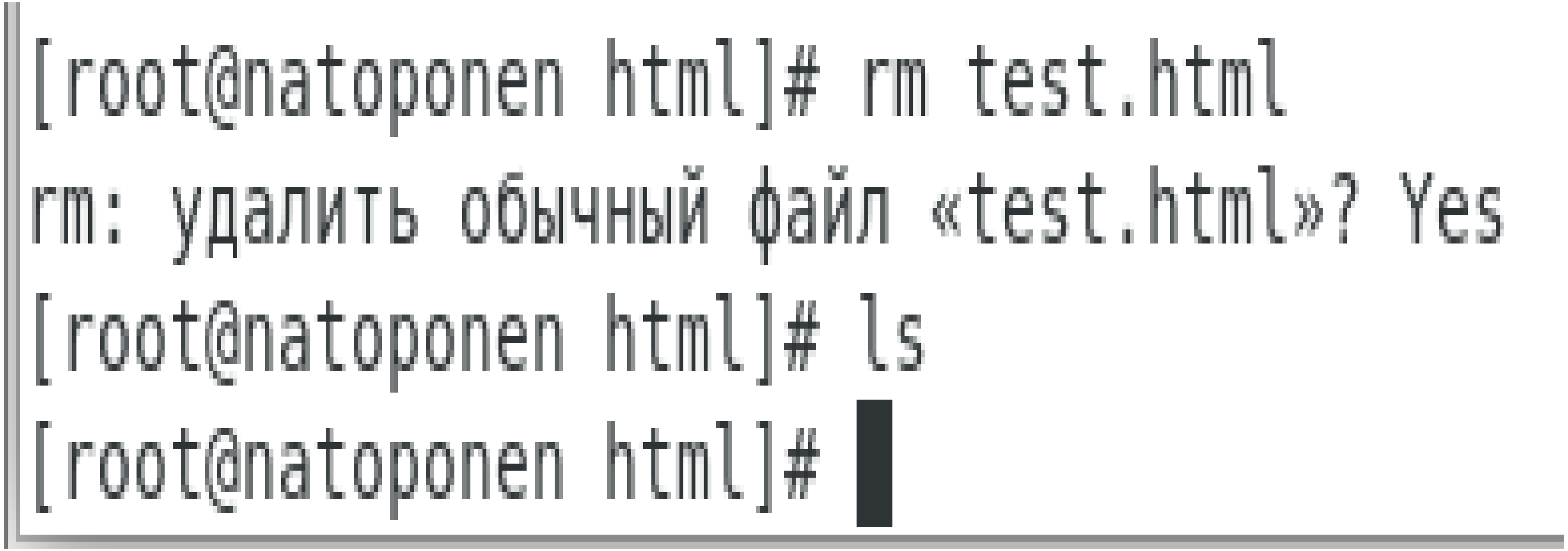
guest@natoponen:/etc/httpd/conf
Файл Правка Вид Поиск Терминал Справка

```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of 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.
#
#Listen 12.34.56.78:80
Listen 80

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding `LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by `httpd -l') do not need
# to be loaded here.
#
-- ВСТАВКА --                                                                                  42,10         9%
```

Рис.18 Возвращение к 80 порту

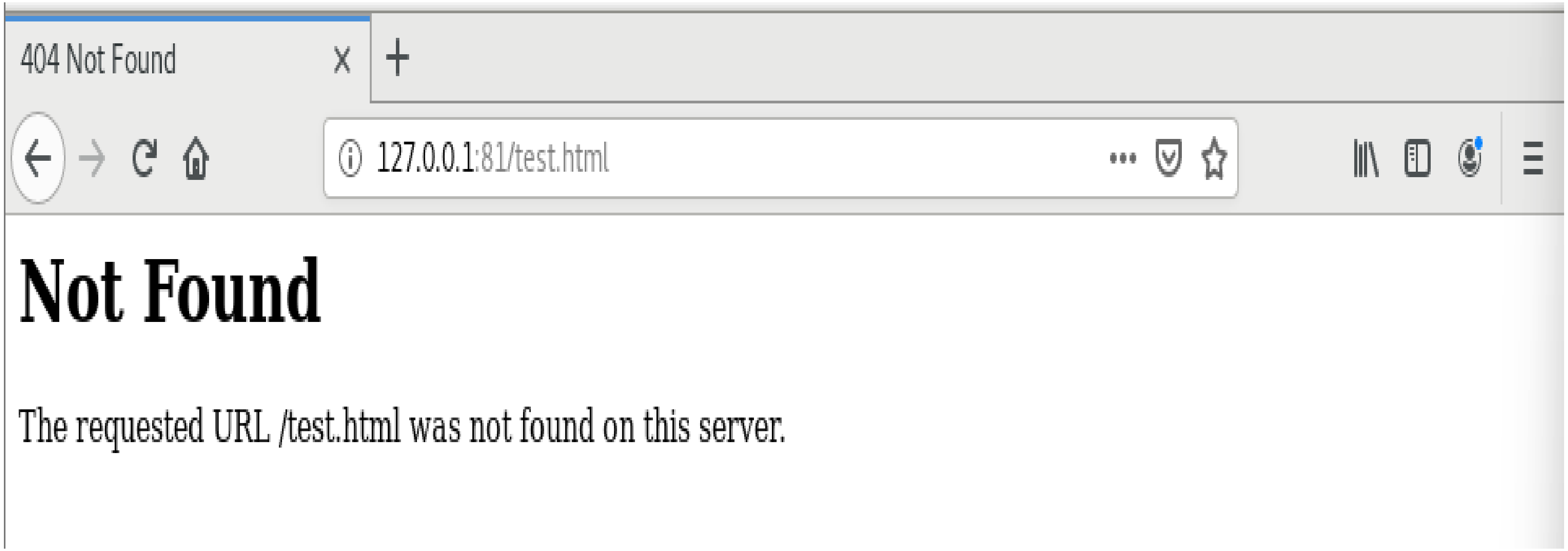
Выполнение работы



```
[root@natoponen html]# rm test.html
rm: удалить обычный файл «test.html»? Yes
[root@natoponen html]# ls
[root@natoponen html]# 
```

Рис.19 Удаление файла страницы

Выполнение работы



Not Found

The requested URL /test.html was not found on this server.

Рис.20 Результат работы сервера после удаления

Выводы

В ходе выполнения данной лабораторной работы я:

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

Спасибо за внимание!