

Лабораторная работа №6

Мандатное разграничение прав в Linux

Топонен Никита Андреевич

Содержание

Цель работы	5
Задание	6
Теоретическое введение	7
Выполнение лабораторной работы	8
Выводы	17
Список литературы	18

Список иллюстраций

1	Режим и политика SELinux	8
2	Запуск Apache web server	9
3	Контекст безопасности Apache web server	9
4	Текущее состояние переключателей SELinux для Apache	10
5	Тип файлов и поддиректорий	10
6	Создание файла test.html	11
7	Контекст файла test.html	11
8	Веб страница	11
9	Контекст файла test.html	11
10	Изменения контекста файла test.html	12
11	Доступ к странице запрещен	12
12	Логи веб сервера	13
13	Audit логи	13
14	Смена порта	14
15	Запуск на 81 порту	14
16	Установка порта	15
17	Работа веб сервера на 81 порту	15
18	Возвращение к 80 порту	16
19	Удаление файла страницы	16
20	Результат работы сервера после удаления	16

Список таблиц

Цель работы

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

Задание

Выполнить задания из лабораторной работы и проанализировать полученные результаты.

Теоретическое введение

Для выполнения данной лабораторной нет специальной теории. Необходимы общие знания в области компьютерных наук.

Выполнение лабораторной работы

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

```
[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

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`.


```
[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 Бс 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

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`

```
[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

Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` Обратите внимание, что многие из них находятся

в положении «off»

```
[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

Определите тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www`

```
[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

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:

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

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

Рис. 6: Создание файла test.html

Проверьте контекст созданного вами файла.

```
[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

Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>.

Убедитесь, что файл был успешно отображён

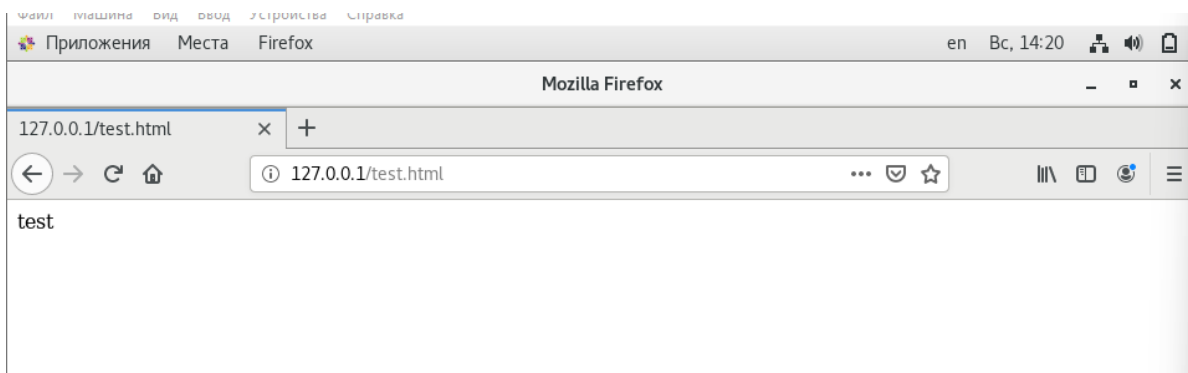


Рис. 8: Веб страница

Проверить контекст файла можно командой `ls -Z. ls -Z /var/www/html/test.html`

```
[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

Измените контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`: `chcon -t samba_share_t /var/www/html/test.html ls -Z /var/www/html/test.html`

```
[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`

Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`



Рис. 11: Доступ к странице запрещен

Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? `ls -l /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.

```

-----
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

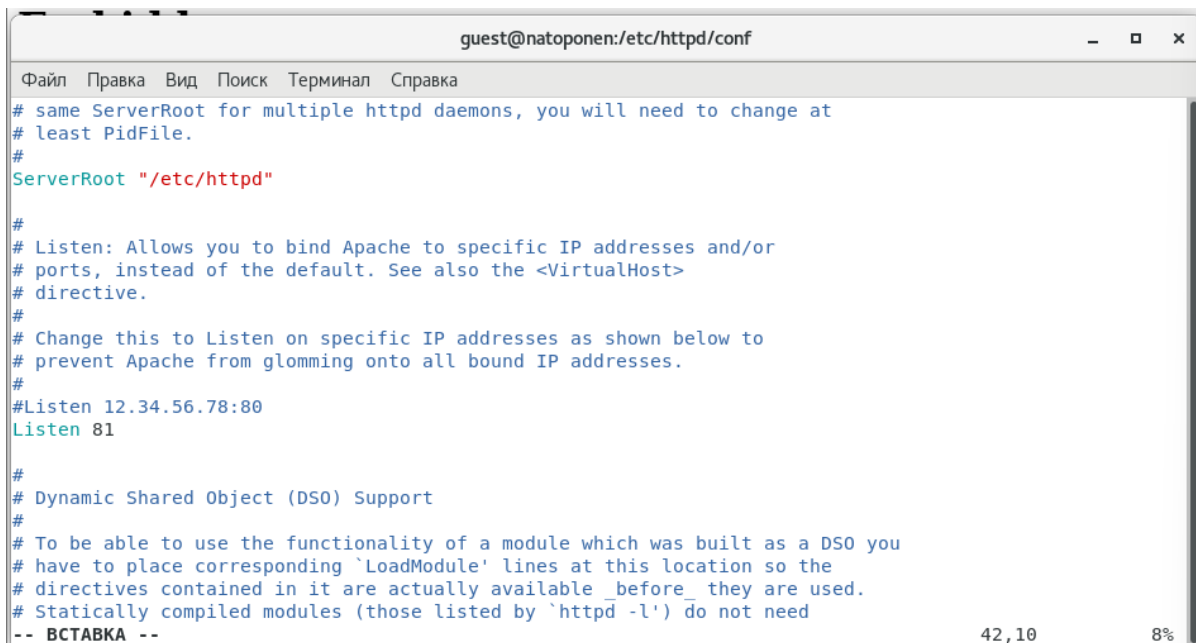
```

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=2F7573722F7362696E2F687474064002D44464F5245475
24F554E44
[root@natoponen html]# █

```

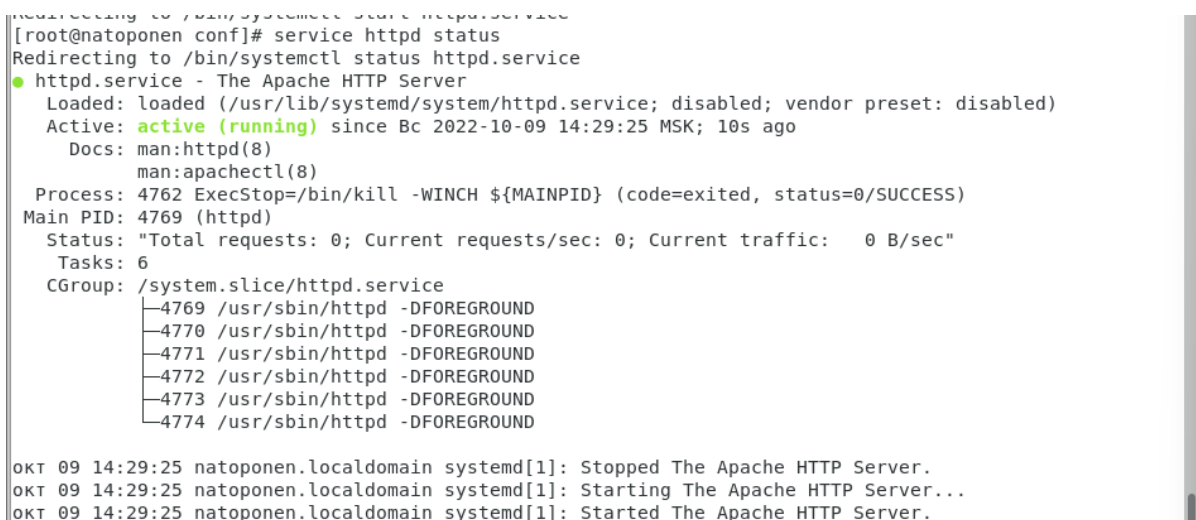
Рис. 13: Audit логи

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.



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



```
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 Бс 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

Сервер успешно запустился на 81 порту.

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`

```
[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

Порт уже был определен.

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».

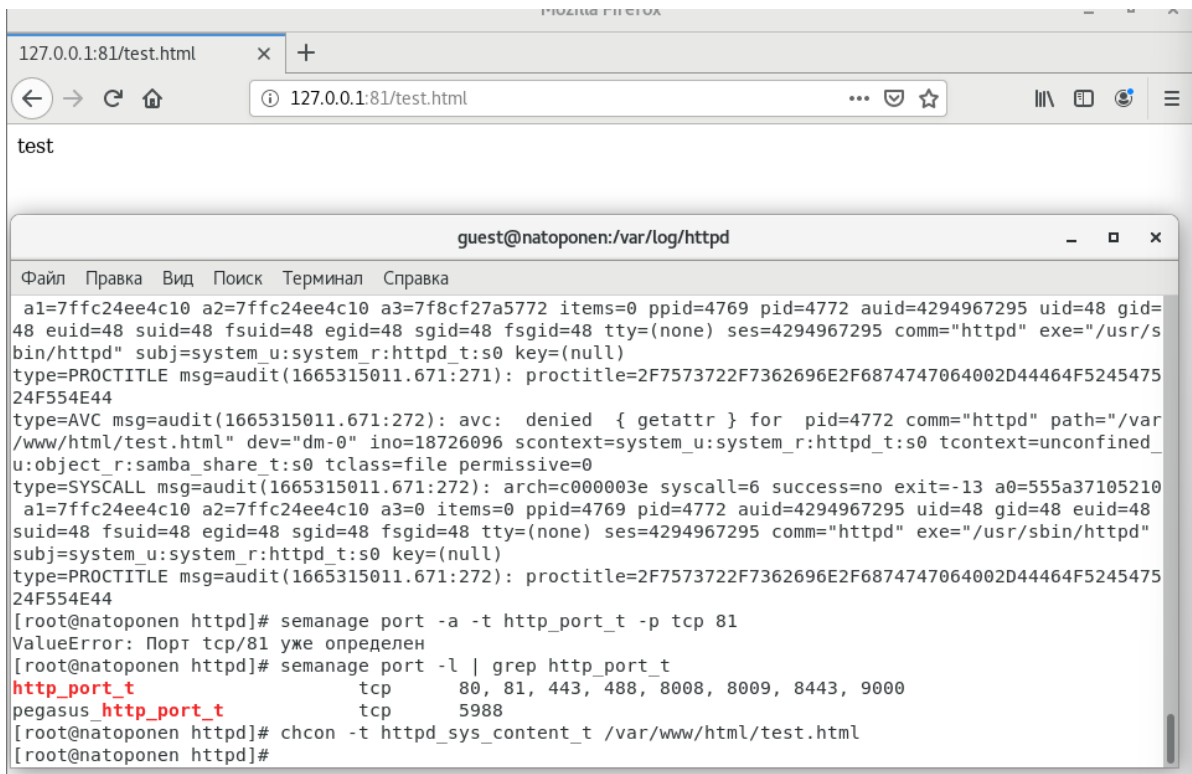


Рис. 17: Работа веб сервера на 81 порту

Исправьте обратно конфигурационный файл `apache`, вернув `Listen 80`.

Удалите привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.

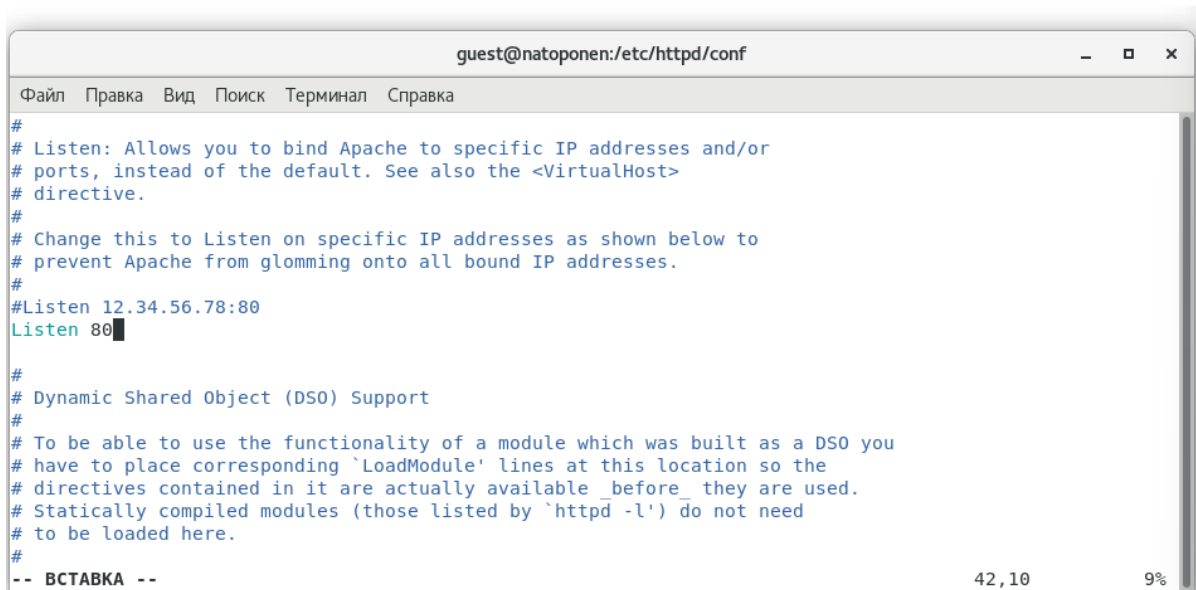


Рис. 18: Возвращение к 80 порту

Удалите файл /var/www/html/test.html: `rm /var/www/html/test.html`

```
[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

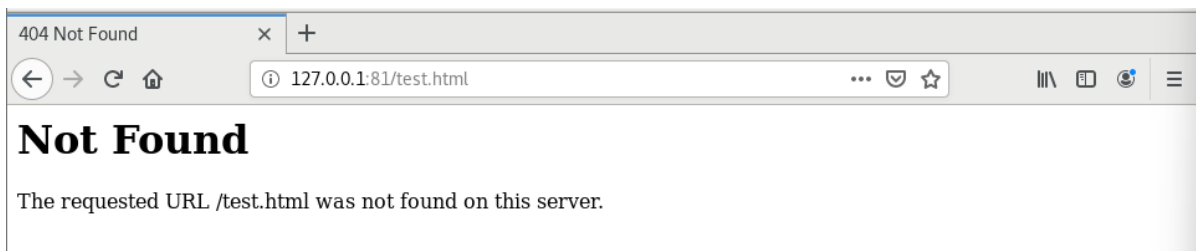


Рис. 20: Результат работы сервера после удаления

Выводы

В ходе данной лабораторной работы я развил навыки администрирования ОС Linux, получил первое практическое знакомство с технологией SELinux, проверил работу SELinux на практике совместно с веб-сервером Apache.

Список литературы

- Кулябов Д. С., Королькова А. В., Геворкян М. Н Лабораторная работа №6