

# Информационная безопасность

Презентация к лабораторной работе  
№\_06

Габриэль Тьерри

# Информация

## Докладчик

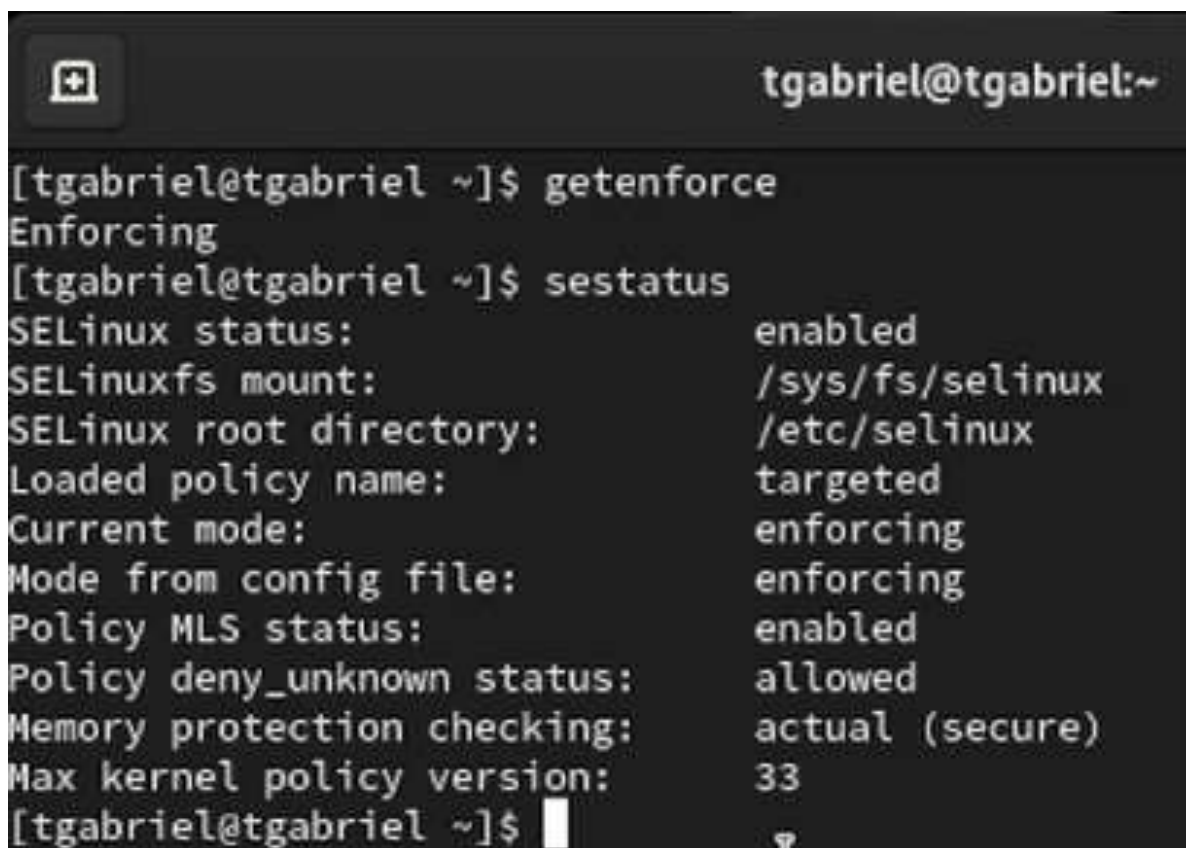
- Габриэль Тьерри
- Студент НКНбд 01-20
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов имени Патриса Лумумбы
- <https://github.com/tgabriel22>
- [1032204249@pfur.ru](mailto:1032204249@pfur.ru)

# Цель работы

- Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1
- Проверить работу SELinux на практике совместно с веб-сервером Apache.

# Выполнение лабораторной работы

1. Вошел в систему под своей учетной записью и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`

A terminal window with a dark background. The title bar shows a window icon and the text 'tgabriel@tgabriel:~'. The terminal content shows the user running 'getenforce' which returns 'Enforcing', and then 'sestatus' which displays a detailed status report for SELinux, including its enabled state, mount points, root directory, loaded policy name (targeted), and current mode (enforcing).

```
[tgabriel@tgabriel ~]$ getenforce
Enforcing
[tgabriel@tgabriel ~]$ 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
[tgabriel@tgabriel ~]$
```

изображение 001

2. Обратился с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедился, что последний работает с помощью команды `service httpd status`

```
[tgabriel@tgabriel ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
• httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Sat 2023-10-14 19:10:22 MSK; 6min ago
     Docs: man:httpd.service(8)
  Main PID: 3017 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0"
    Tasks: 213 (limit: 12146)
   Memory: 33.3M
      CPU: 583ms
    CGroup: /system.slice/httpd.service
            └─3017 /usr/sbin/httpd -DFOREGROUND
              └─3018 /usr/sbin/httpd -DFOREGROUND
                └─3022 /usr/sbin/httpd -DFOREGROUND
                  └─3023 /usr/sbin/httpd -DFOREGROUND
                    └─3025 /usr/sbin/httpd -DFOREGROUND

Oct 14 19:10:22 tgabriel.localdomain systemd[1]: Starting The Apache HTTP Server:
Oct 14 19:10:22 tgabriel.localdomain systemd[1]: Started The Apache HTTP Server.
Oct 14 19:10:22 tgabriel.localdomain httpd[3017]: Server configured, listening on:
[tgabriel@tgabriel ~]$
```

### 3. Определил контекст безопасности веб-сервера Apache - httpd\_t С помощью команды ps auxZ | grep httpd

```
[tgabriel@tgabriel ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root      3017   0.0  0.5  20328 11660 ?
Ss   19:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3018   0.0  0.3   2164   7540 ?
S    19:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3022   0.0  0.8 1210612 17220 ?
Sl   19:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3023   0.0  0.6 1079476 13132 ?
Sl   19:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3025   0.0  0.7 1079476 15176 ?
Sl   19:10   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 tgabriel 3373 0.0  0.1 221
664 2236 pts/0 S+ 19:17   0:00 grep --color=auto httpd
[tgabriel@tgabriel ~]$
```

изображение 003

4. Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b httpd`, многие из переключателей находятся в положении off

```
[tgabriel@tgabriel ~]$ 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
Memory protection checking:    actual (secure)
Max kernel policy version:     33

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
```

изображение 004

5. Посмотрел статистику по политике с помощью команды seinfo, также определите множество пользователей, ролей, типов.
6. Посмотрел тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды ls -lZ /var/www
7. Определил тип файлов, находящихся в директории /var/www/html: ls -lZ /var/www/html
8. Определил круг пользователей, которым разрешено создание файлов в директории /var/www/html.

```
[tgabriel@tgabriel ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 23
:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 May 16 23
:21 html
[tgabriel@tgabriel ~]$ ls -lZ /var/www/html
total 0
```

изображение 005



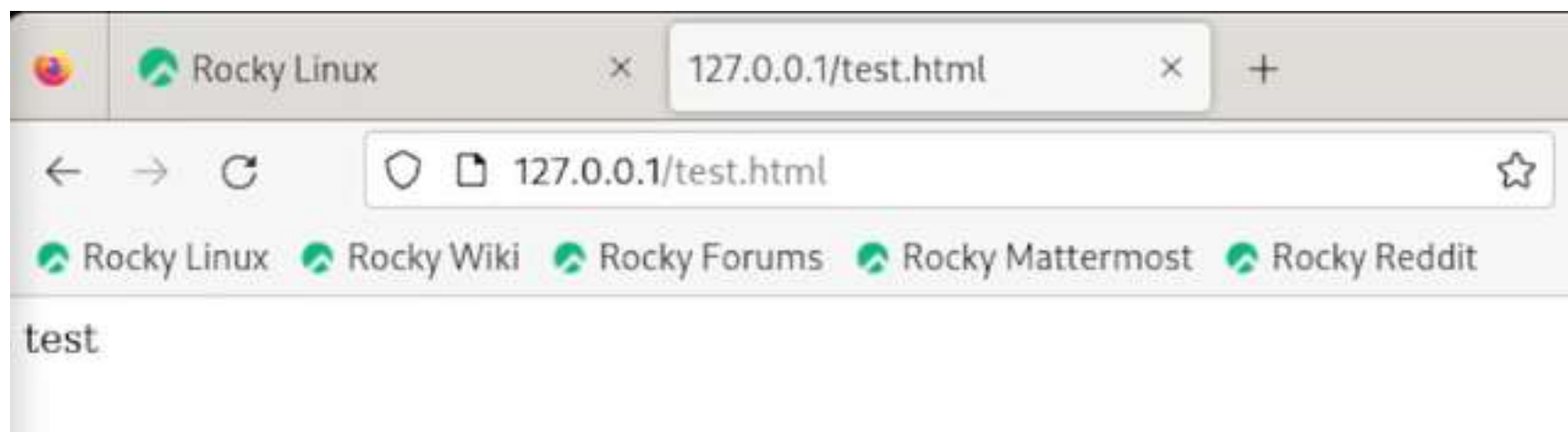
9. создал от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания:

test

```
[tgabriel@tgabriel ~]$ su
Password:
[root@tgabriel tgabriel]# touch /var/www/html/test.html
[root@tgabriel tgabriel]# vim /var/www/html/test.html
[root@tgabriel tgabriel]# cat /var www/html/test.html
cat: /var: Is a directory
cat: www/html/test.html: No such file or directory
[root@tgabriel tgabriel]# cat /var/www/html/test.html
<html>
    <body>test</body>
</html>
```

10.Проверил контекст созданного вами файла.

11.Обратился к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`.  
убедился, что файл был успешно отображён.



изображение 007

12. Изучил справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставил их с типом файла `test.html`. Проверил контекст файла можно командой `ls -Z`. `ls -Z /var/www/html/test.html`
13. Изменил 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` После этого проверил, что контекст поменялся.

```
[root@tgabriel tgabriel]# man httpd_selinux
No manual entry for httpd_selinux
[root@tgabriel tgabriel]# ls -z /var/www/html/test.html
ls: invalid option -- 'z'
Try 'ls --help' for more information.
[root@tgabriel tgabriel]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@tgabriel tgabriel]# chcon -t samba_share_t /var/www/html/test.html
[root@tgabriel tgabriel]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@tgabriel tgabriel]#
```

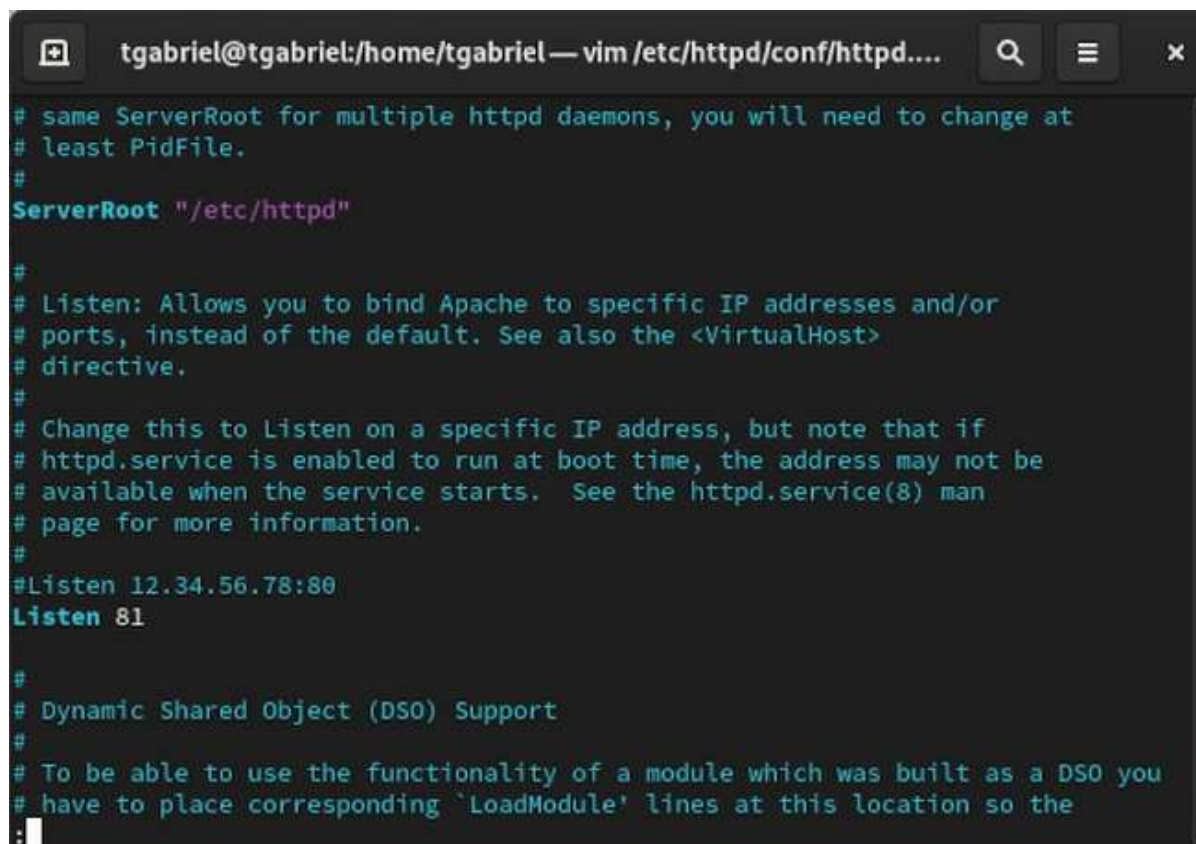
14. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. и получил сообщение об ошибке: Forbidden You don't have permission to access /test.html on this server.



изображение 009

15. Проанализировал ситуацию. Просмотрел log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail /var/log/messages`
16. Попробовал 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`.

```
[root@tgabriel tgabriel]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 34 Oct 14 19:27 /var/www/html/test.html
[root@tgabriel tgabriel]# tail /var/log/messages
Oct 14 19:54:13 tgabriel gnome-shell[1689]: libinput error: event5 - VirtualBox
mouse integration: client bug: event processing lagging behind by 21ms, your sy
stem is too slow
Oct 14 19:54:16 tgabriel systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootP
rivileged@0.service: Deactivated successfully.
Oct 14 19:54:16 tgabriel systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootP
rivileged@0.service: Consumed 4.746s CPU time.
Oct 14 19:54:16 tgabriel systemd[1]: setroubleshootd.service: Deactivated succes
sfully.
Oct 14 19:54:16 tgabriel systemd[1]: setroubleshootd.service: Consumed 4.391s CP
U time.
Oct 14 19:54:32 tgabriel systemd[1]: Starting dnf makecache...
Oct 14 19:54:37 tgabriel dnf[4362]: Metadata cache refreshed recently.
Oct 14 19:54:37 tgabriel systemd[1]: dnf-makecache.service: Deactivated successf
ully.
Oct 14 19:54:38 tgabriel systemd[1]: Finished dnf makecache.
Oct 14 19:54:38 tgabriel systemd[1]: dnf-makecache.service: Consumed 2.127s CPU
time.
[root@tgabriel tgabriel]# vim /etc/httpd/http.conf
[root@tgabriel tgabriel]# vim /etc/http.conf
[root@tgabriel tgabriel]# vim /etc/httpd/conf/httpd.conf
```



```
tgabriel@tgabriel:/home/tgabriel — vim /etc/httpd/conf/httpd....
# 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 a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#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
#
```

изображение 011

17.Выполнил перезапуск веб-сервера Apache.

18.Проанализовал лог-файлы: tail -n1  
/var/log/messages Просмотрел файлы  
/var/log/http/error\_log, /var/log/http/access\_log и  
/var/log/audit/audit.log и выясните, в каких файлах  
появились записи.

```
[root@tgabriel tgabriel]# tail -n1 /var/log/httpd/error_log
[Sat Oct 14 19:53:41.914934 2023] [core:error] [pid 4217:tid 4272] (13)Permissio
n denied: [client 127.0.0.1:56766] AH00035: access to /test.html denied (filesys
tem path '/var/www/html/test.html') because search permissions are missing on a
component of the path
[root@tgabriel tgabriel]# tail -n1 /var/log/httpd/access_log
127.0.0.1 - - [14/Oct/2023:19:53:41 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
[root@tgabriel tgabriel]# tail -n1 /var/log/audit/audit.log
type=SERVICE_STOP msg=audit(1697302478.008:238): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="system
d" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'UID=
"root" AUID="unset"
```

изображение 012

19.Выполнил команду `semanage port -a -t http_port_t -p tcp 81` После этого проверьте список портов командой `semanage port -l | grep http_port_t` убедился, что порт 81 появился в списке.

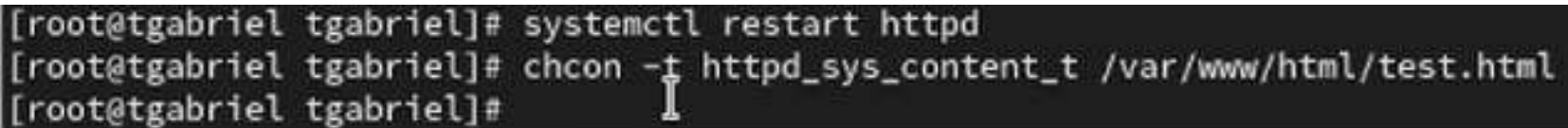
```
[root@tgabriel tgabriel]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@tgabriel tgabriel]# semanage port -l | grep http_port_t
semanage port: error: one of the arguments -a/--add -d/--delete -m/--modify -l/--list -E/--extract -D/--deleteall is required
[root@tgabriel tgabriel]# 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@tgabriel tgabriel]#
```

изображение 013



20. Попробовал запустить веб-сервер Apache ещё раз

20. Вернул 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 Попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. и увидел содержимое файла — слово «test».

A terminal window with a dark background and light gray text. It shows three lines of commands entered at the root prompt of a machine named 'tgabriel'. The first line is 'systemctl restart httpd'. The second line is 'chcon -t httpd\_sys\_content\_t /var/www/html/test.html'. The third line is an empty prompt. A cursor is visible at the end of the third line.

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

изображение 014

## 22.Исправил обратно конфигурационный файл apache, вернув Listen 80.

```
#  
# 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 a specific IP address, but note that if  
# httpd.service is enabled to run at boot time, the address may not be  
# available when the service starts. See the httpd.service(8) man  
# page for more information.  
#  
#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.  
#  
# Example:  
-- INSERT --
```

47,10

10%

изображение 015

23. Удалил привязку http\_port\_t к 81 порту:  
semanage port -d -t http\_port\_t -p tcp 81 и  
проверил, что порт 81 удалён.

24. Удалил файл /var/www/html/test.html: rm  
/var/www/html/test.html

```
[root@tgabriel tgabriel]# vim /etc/httpd/conf/httpd.conf
[root@tgabriel tgabriel]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@tgabriel tgabriel]# 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@tgabriel tgabriel]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@tgabriel tgabriel]#
```

изображение 016

# Выводы

- Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1
- Проверить работу SELinx на практике совместно с веб-сервером Apache.