

# Отчет по лабораторной работе №6

---

Перельгин Сергей Викторович

## Цель работы

---

## Цель лабораторной работы

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

# **Выполнение лабораторной работы**

---

С помощью команд `getenforce` и `sestatus` убедился, что SELinux работает в режиме enforcing политики targeted (рис. 1).

A terminal window with a dark background. The title bar shows a window icon and the text "sergeiperel@fedora:~". The terminal content shows the execution of two commands: "getenforce" and "sestatus". The output of "getenforce" is "Enforcing". The output of "sestatus" is a multi-line status report. The terminal text is as follows:

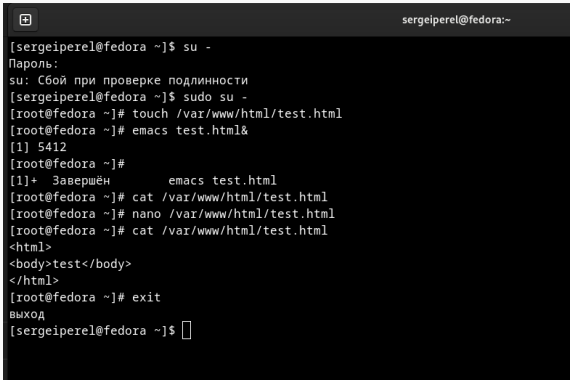
```
[sergeiperel@fedora ~]$ getenforce
Enforcing
[sergeiperel@fedora ~]$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:           targeted
Current mode:                 enforcing
Mode from config file:       enforcing
Policy MLS status:           enabled
Policy deny_unknown status:   allowed
Memory protection checking:   actual (secure)
Max kernel policy version:    33
[sergeiperel@fedora ~]$
```

**Рис. 1:** Проверка режима enforcing политики targeted

Обратился с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедился, что последний работает с помощью команды “service httpd status”. С помощью команды “ps auxZ | grep httpd” определил контекст безопасности веб-сервера Apache - httpd\_t. Посмотрел текущее состояние переключателей SELinux и статистику по политике с помощью команды “seinfo”.

# Создание основного файла

От имени суперпользователя создал html-файл  
/var/www/html/test.html (рис. 2).

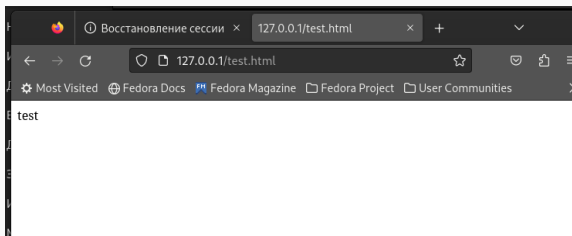
A terminal window with a dark background and light text. The title bar shows a window icon and the text 'sergeiperel@fedora:~'. The terminal content shows a user switching to root via 'su -', creating a file with 'touch', editing it with 'emacs', and finally exiting root with 'exit'.

```
[sergeiperel@fedora ~]$ su -  
Пароль:  
su: Сбой при проверке подлинности  
[sergeiperel@fedora ~]$ sudo su -  
[root@fedora ~]# touch /var/www/html/test.html  
[root@fedora ~]# emacs test.html&  
[1] 5412  
[root@fedora ~]#  
[1]+  Завершён      emacs test.html  
[root@fedora ~]# cat /var/www/html/test.html  
[root@fedora ~]# nano /var/www/html/test.html  
[root@fedora ~]# cat /var/www/html/test.html  
<html>  
<body>test</body>  
</html>  
[root@fedora ~]# exit  
ВЫХОД  
[sergeiperel@fedora ~]$
```

**Рис. 2:** Создание файла /var/www/html/test.html

# Просмотр файла в веб-браузере

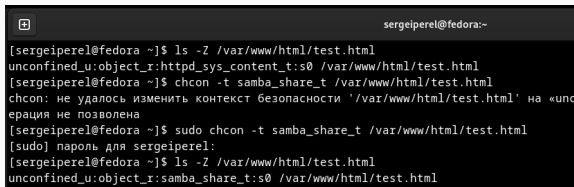
Обратился к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”. Файл был успешно отображен (рис. 3).



**Рис. 3:** Обращение к файлу через веб-сервер



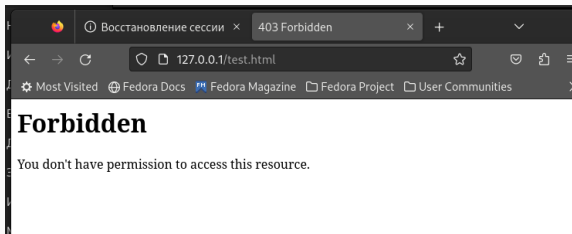
Изменил контекст файла на `samba_share_t` командой “`sudo chcon -t samba_share_t /var/www/html/test.html`” и проверил, что контекст поменялся (рис. 4).



```
sergeiperel@fedora:~  
[sergeiperel@fedora ~]$ ls -Z /var/www/html/test.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[sergeiperel@fedora ~]$ chcon -t samba_share_t /var/www/html/test.html  
chcon: не удалось изменить контекст безопасности '/var/www/html/test.html' на «unc  
ерация не позволена  
[sergeiperel@fedora ~]$ sudo chcon -t samba_share_t /var/www/html/test.html  
[sudo] пароль для sergeiperel:  
[sergeiperel@fedora ~]$ ls -Z /var/www/html/test.html  
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

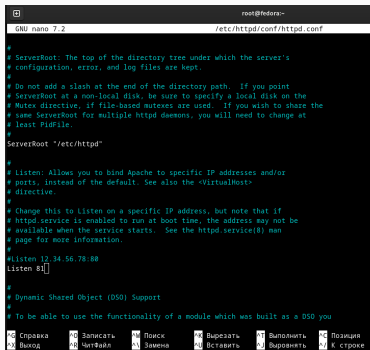
Рис. 4: Изменение контекста

Попробовал еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html” и получил сообщение об ошибке (т.к. к установленному ранее контексту процесс httpd не имеет доступа) (рис. 5).



**Рис. 5:** Обращение к файлу через веб-сервер

В файле `/etc/httpd/conf/httpd.conf` заменил строчку “Listen 80” на “Listen 81”, чтобы установить веб-сервер Apache на прослушивание TCP-порта 81 (рис. 6).

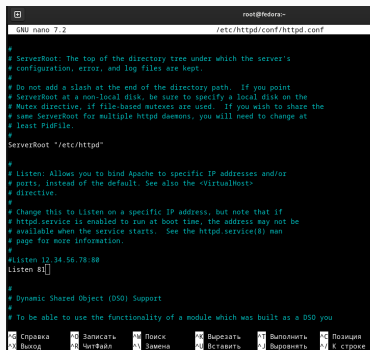


```
root@fedora:~  
GNU nano 7.2 /etc/httpd/conf/httpd.conf  
  
#  
# ServerRoot: The top of the directory tree under which the server's  
# configuration, error, and log files are kept.  
#  
# Do not add a slash at the end of the directory path. If you point  
# ServerRoot at a non-local disk, be sure to specify a local disk on the  
# Mutex directive, if file-based mutexes are used. If you wish to share the  
# 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
```

**Рис. 6:** Установка веб-сервера Apache на прослушивание TCP-порта 81

# Повторный просмотр в веб-браузере

Вернул контекст “httpd\_sys\_content\_t” файлу “/var/www/html/test.html” и после этого попробовал получить доступ к файлу через веб-сервер, введя адрес “http://127.0.0.1:81/test.html”, в результате чего увидел содержимое файла - слово “test” (рис. 7).



```
root@fedora:~  
GNU nano 7.2 /etc/httpd/conf/httpd.conf  
  
#  
# ServerRoot: The top of the directory tree under which the server's  
# configuration, error, and log files are kept.  
#  
# Do not add a slash at the end of the directory path. If you point  
# ServerRoot to a non-local disk, be sure to specify a local disk on the  
# Mutex directive, if file-based mutexes are used. If you wish to share the  
# 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
```

Справка	Записать	Поиск	Вырезать	Выполнить	Позиция
Выход	Чит-файл	Замена	Вставить	Выровнять	К строке

Рис. 7: Обращение к файлу через веб-сервер

## Завершение лабораторной работы

Исправил обратно конфигурационный файл apache, вернув “Listen 80”. Попытался удалить привязку http\_port к 81 порту командой “semanage port -d -t http\_port\_t -p tcp 81”, но этот порт определен на уровне политики, поэтому его нельзя удалить. Удалил файл “/var/www/html/test.html” командой “rm /var/www/html/test.html” (рис. 8).

```
[root@fedora ~]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? yes
[root@fedora ~]# ls /var/www/html/
[root@fedora ~]#
```

**Рис. 8:** Удаление файла test.html

## Выводы

---

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

Спасибо за внимание!