

# **Мандатное разграничение прав в Linux**

**Лабораторная работа №6**

Тарутина Кристина Олеговна

# Содержание

|          |                                       |           |
|----------|---------------------------------------|-----------|
| <b>1</b> | <b>Цель работы</b>                    | <b>5</b>  |
| <b>2</b> | <b>Выполнение лабораторной работы</b> | <b>6</b>  |
| <b>3</b> | <b>Выводы</b>                         | <b>10</b> |
|          | <b>Список литературы</b>              | <b>11</b> |

## Список иллюстраций

|     |                            |   |
|-----|----------------------------|---|
| 2.1 | Название рисунка . . . . . | 6 |
| 2.2 | Название рисунка . . . . . | 7 |
| 2.3 | Название рисунка . . . . . | 7 |
| 2.4 | Название рисунка . . . . . | 7 |
| 2.5 | Название рисунка . . . . . | 8 |
| 2.6 | Название рисунка . . . . . | 8 |
| 2.7 | Название рисунка . . . . . | 9 |
| 2.8 | Название рисунка . . . . . | 9 |

## Список таблиц

# 1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux

Проверить работу SELinux на практике совместно с веб-сервером Apache.

## 2 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`. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status` Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www` (рис. 2.1).

```
(kotarutina@kotarutina)-[~]
$ getenforce
Enforcing

(kotarutina@kotarutina)-[~]
$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            default
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

(kotarutina@kotarutina)-[~]
$ service httpd status

Unit httpd.service could not be found.

(kotarutina@kotarutina)-[~]
$ ls -lZ /var/www
total 4
drwxr-xr-x. 3 root root system_u:object_r:httpd_sys_content_t:s0 4096 Apr 27
14:48 html
```

Рис. 2.1: Название рисунка

Определите тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html` Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html` (рис. 2.2).

```

(kotarutina@kotarutina)-[~]
$ ls -lZ /var/www
total 4
drwxr-xr-x. 3 root root system_u:object_r:httpd_sys_content_t:s0 4096 Apr 27
14:48 html

(kotarutina@kotarutina)-[~]
$ ls -lZ /var/www/html
total 20
drwxrwxrwx. 12 root root system_u:object_r:httpd_sys_content_t:s0 4096 Apr 2
7 14:48 DVWA
-rw-r--r--. 1 root root system_u:object_r:httpd_sys_content_t:s0 10701 Apr 2
6 21:18 index.html
-rw-r--r--. 1 root root system_u:object_r:httpd_sys_content_t:s0 615 Apr 2
6 21:20 index.nginx-debian.html

```

Рис. 2.2: Название рисунка

Создайте от имени суперпользователя (так как в дистрибутиве после установ-  
ки только ему разрешена запись в директорию) html-файл `/var/www/html/test.html`  
следующего содержания:

test

(рис. 2.3).

```

(kotarutina@kotarutina)-[~]
$ sudo chmod 777 /var/www/html/test.html

(kotarutina@kotarutina)-[~]
$ mcedit /var/www/html/test.html

```

Рис. 2.3: Название рисунка

Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`.  
Убедитесь, что файл был успешно отображён Тут, к сожалению, по какой-то  
причине у меня отказался запускаться firefox (рис. 2.4).

```

(kotarutina@kotarutina)-[~]
$ firefox
ExceptionHandler::GenerateDump cloned child 10955
ExceptionHandler::SendContinueSignalToChild sent continue signal to child
ExceptionHandler::WaitForContinueSignal waiting for continue signal...

```

Рис. 2.4: Название рисунка

Изучите справку `man httpd_selinux` и выясните, какие контексты файлов опре-  
делены для httpd. Сопоставьте их с типом файла `test.html`. Проверить контекст  
файла можно командой `ls -Z. ls -Z /var/www/html/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` (рис. 2.5).

```
(kotarutina@kotarutina)-[~]
$ man httpd_selinux
No manual entry for httpd_selinux

(kotarutina@kotarutina)-[~]
$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html

(kotarutina@kotarutina)-[~]
$ chcon -t samba_share_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:samba_share_t:s0': Operation not permitted

(kotarutina@kotarutina)-[~]
$ sudo chcon -t samba_share_t /var/www/html/test.html

(kotarutina@kotarutina)-[~]
$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Рис. 2.5: Название рисунка

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. (рис. 2.6).

```
(kotarutina@kotarutina)-[~]
$ sudo chcon -t samba_share_t /var/www/html/test.html

(kotarutina@kotarutina)-[~]
$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html

(kotarutina@kotarutina)-[~]
$ ls -l /var/www/html/test.html
-rwxrwxrwx. 1 root root 32 Apr 27 21:27 /var/www/html/test.html

(kotarutina@kotarutina)-[~]
```

Рис. 2.6: Название рисунка

Проанализируйте лог-файлы: `tail -nl /var/log/messages` Просмотрите файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` и выясните, в каких файлах появились записи. 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` Убедитесь, что порт 81 появился в списке. Попробуйте запустить веб-сервер Apache ещё (рис. 2.7).

```
(kotarutina@kotarutina)~]
$ tail /var/log/messages

tail: cannot open '/var/log/messages' for reading: No such file or directory

(kotarutina@kotarutina)~]
$ semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
               {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,permissive,dontaudit}
               ...
semanage: error: unrecognized arguments: -p 81

(kotarutina@kotarutina)~]
$ semanage port -l | grep http_port_t
```

Рис. 2.7: Название рисунка

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». 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. Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html` (рис. 2.8).

```
(kotarutina@kotarutina)~]
$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html

(kotarutina@kotarutina)~]
$ rm /var/www/html/test.html
rm: cannot remove '/var/www/html/test.html': Permission denied

(kotarutina@kotarutina)~]
$ sudo rm /var/www/html/test.html

(kotarutina@kotarutina)~]
$
```

Рис. 2.8: Название рисунка

## 3 Выводы

Мы успешно развили навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux

Проверили работу SELinux на практике совместно с веб-сервером Apache.

## **Список литературы**