

Лабораторная работа №6

Мандатное разграничение прав в Linux

Карымшаков Артур Алишерович

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	15
5	Список литературы	16

Список таблиц

Список иллюстраций

3.1	Проверка режима работы SELinux	7
3.2	Проверка работы веб-сервера	8
3.3	Поиск веб-сервера Apache и определение его контекста безопасности	8
3.4	Текущее состояние переключателей SELinux для Apache	9
3.5	Определение типов файлов и поддиректорий, находящихся в директории /var/www	9
3.6	Определение типов файлов и поддиректорий, находящихся в директории /var/www/html	10
3.7	html-файл и его содержимое	10
3.8	Контекст html-файл	10
3.9	Выяснение контекста файла	11
3.10	Изменение контекста файла	11
3.11	Попытка получить доступ к файлу через веб-сервер	11
3.12	Просмотр системного лог-файла	12
3.13	Просмотр портов	12
3.14	Возвращение исходного контекста	12
3.15	Получение доступа к файлу через веб-сервер	13
3.16	Возвращение строки Listen 80	13
3.17	Удаление файла /var/www/html/test.html	14

1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. [1]

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

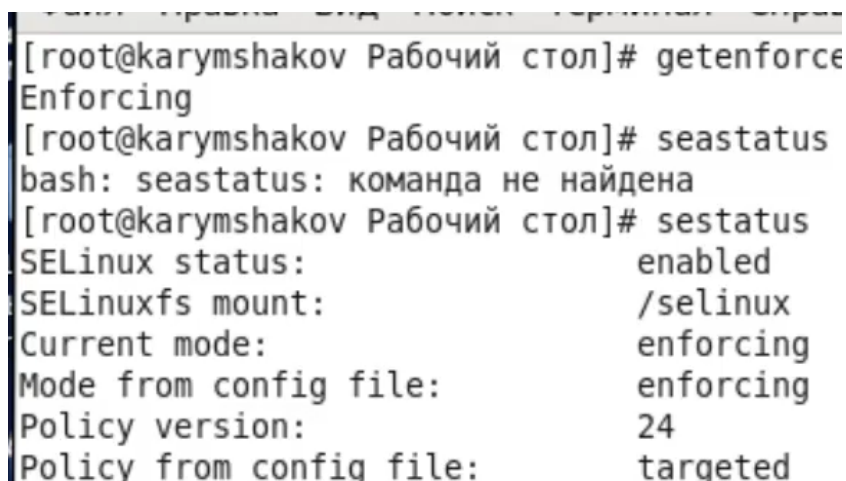
2 Задание

1. С помощью различных примеров ознакомиться с работой SELinux и веб-сервисом Apache.

3 Выполнение лабораторной работы

1. С помощью различных примеров ознакомился с работой SELinux и веб-сервисом Apache.

Вошел в систему с полученными учетными данными и убедился, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus` (рис - @fig:005).



```
[root@karymshakov Рабочий стол]# getenforce
Enforcing
[root@karymshakov Рабочий стол]# seastatus
bash: seastatus: команда не найдена
[root@karymshakov Рабочий стол]# sestatus
SELinux status:                enabled
SELinuxfs mount:              /selinux
Current mode:                  enforcing
Mode from config file:         enforcing
Policy version:                24
Policy from config file:       targeted
```

Рис. 3.1: Проверка режима работы SELinux

Обратится с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедился, что последний работает с помощью команды `/etc/rc.d/init.d/httpd status`, предварительно запустив его с помощью команды `/etc/rc.d/init.d/httpd start` (рис - @fig:006).

```

[root@karymshakov Рабочий стол]# service httpd status
httpd остановлен
[root@karymshakov Рабочий стол]# start /etc/rc.d/init.d/httpd status
start: Unknown job: /etc/rc.d/init.d/httpd
[root@karymshakov Рабочий стол]# start /etc/rc.d/init.d/httpd
start: Unknown job: /etc/rc.d/init.d/httpd
[root@karymshakov Рабочий стол]# /etc/rc.d/init.d/httpd start
Запускается httpd: httpd: apr_sockaddr_info_get() failed for karymshakov.localdomain
main
httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 for ServerName
[ OK ]
[root@karymshakov Рабочий стол]#

```

Рис. 3.2: Проверка работы веб-сервера

Нашел веб-сервер Apache в списке процессов и определил его контекст безопасности с помощью команды `ps auxZ | grep httpd` (рис - @fig:007).

```

[root@karymshakov Рабочий стол]# ps auxZ | grep httpd
unconfined_u:system_r:httpd_t:s0 root      2602  0.0  0.3 12180 3544 ?        Ss
19:32   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  2605  0.0  0.2 12180 2184 ?        Ss
19:32   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  2606  0.0  0.2 12180 2184 ?        Ss
19:32   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  2607  0.0  0.2 12180 2184 ?        Ss
19:32   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  2608  0.0  0.2 12180 2184 ?        Ss
19:32   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  2609  0.0  0.2 12180 2184 ?        Ss
19:32   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  2610  0.0  0.2 12180 2184 ?        Ss
19:32   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  2611  0.0  0.2 12180 2184 ?        Ss
19:32   0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache  2612  0.0  0.2 12180 2184 ?        Ss
19:32   0:00 /usr/sbin/httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 2615  0.0  0.0 4376 784 pts/0 S+ 19:32   0:00 grep httpd
[root@karymshakov Рабочий стол]#

```

Рис. 3.3: Поиск веб-сервера Apache и определение его контекста безопасности

Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b` (рис - @fig:008). Многие из них находятся в положении “off”.

Файл	Правка	Вид	Поиск	Терминал	Справка
httpd_can_network_connect_db					off
httpd_can_network_memcache					off
httpd_can_network_relay					off
httpd_can_sendmail					off
httpd_dbus_avahi					on
httpd_dbus_sssd					off
httpd_enable_cgi					on
httpd_enable_ftp_server					off
httpd_enable_homedirs					off
httpd_execmem					off
httpd_manage_ipa					off
httpd_read_user_content					off
httpd_run_preupgrade					off
httpd_run_stickshift					off
httpd_serve_cobbler_files					off
httpd_setrlimit					off
httpd_ssi_exec					off
httpd_tmp_exec					off
httpd_tty_comm					on
httpd_unified					on
httpd_use_cifs					off
httpd_use_fusefs					off
httpd_use_gpg					off
httpd_use_nfs					off

Рис. 3.4: Текущее состояние переключателей SELinux для Apache

Определил тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www` (рис - @fig:010).

```
[root@karymshakov Рабочий стол]# ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 error
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 icons
[root@karymshakov Рабочий стол]# ls -lZ /var/www/html
[root@karymshakov Рабочий стол]# ls -lZ /var/www/html
```

Рис. 3.5: Определение типов файлов и поддиректорий, находящихся в директории /var/www

Определил тип файлов, находящихся в директории /var/www/html с помощью команды `ls -lZ /var/www/html` (рис - @fig:011).

```
[root@karymshakov Рабочий стол]# ls -lZ /var/www/html
[root@karymshakov Рабочий стол]# ls -lZ /var/www/html
```

Рис. 3.6: Определение типов файлов и поддиректорий, находящихся в директории /var/www/html

Консоль ничего не выводит, поскольку директория пуста.

Создал от имени суперпользователя html-файл /var/www/html/test.html следующего содержания (рис - @fig:013):

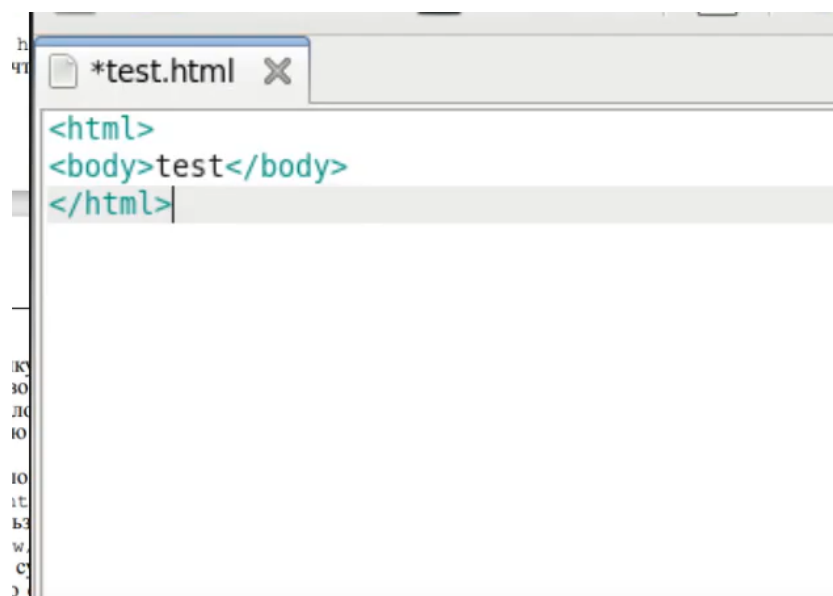


Рис. 3.7: html-файл и его содержимое

Проверил контекст созданного мною файла (рис - @fig:014):

```
/share/recently-used.xbel', but failed: Нет такого файла или каталога
[root@karymshakov Рабочий стол]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t /var/www/html
/test.html
[root@karymshakov Рабочий стол]#
```

Рис. 3.8: Контекст html-файл

Проверил контекст файла с помощью команды `ls -Z /var/www/html/test.html` (рис - @fig:016).

```
[root@karymshakov Рабочий стол]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@karymshakov Рабочий стол]# chcon -t samba_share_t /var/www/html/test.html
```

Рис. 3.9: Выяснение контекста файла

Изменил контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t` (рис - @fig:017).

```
[root@karymshakov Рабочий стол]# chcon -t samba_share_t /var/www/html/test.html
[root@karymshakov Рабочий стол]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Рис. 3.10: Изменение контекста файла

Попробовал еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получил ошибку (рис - @fig:018).

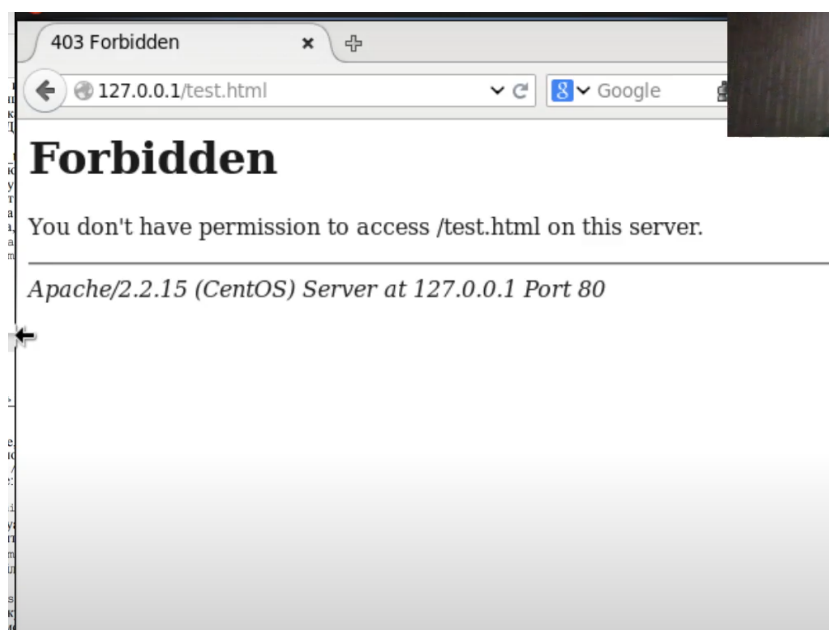


Рис. 3.11: Попытка получить доступ к файлу через веб-сервер

Проанализировал ситуацию. Просмотрел log-файлы веб-сервера Apache, а также посмотрел системный лог-файл с помощью команды `tail /var/log/messages` (рис - @fig:019).

```
[root@karymshakov Рабочий стол]# tail /var/log/messages
Feb 19 19:09:38 karymshakov NetworkManager[1238]: <info> gateway 10.0.2.2
Feb 19 19:09:38 karymshakov NetworkManager[1238]: <info> nameserver '192.168.0
.1'
Feb 19 19:09:38 karymshakov NetworkManager[1238]: <info> Activation (eth0) Stage
5 of 5 (IP Configure Commit) scheduled...
Feb 19 19:09:38 karymshakov NetworkManager[1238]: <info> Activation (eth0) Stage
4 of 5 (IP4 Configure Get) complete.
Feb 19 19:09:38 karymshakov NetworkManager[1238]: <info> Activation (eth0) Stage
5 of 5 (IP Configure Commit) started...
Feb 19 19:09:38 karymshakov dhclient[2296]: bound to 10.0.2.15 -- renewal in 350
27 seconds.
Feb 19 19:09:39 karymshakov NetworkManager[1238]: <info> (eth0): device state ch
ange: ip-config -> activated (reason 'none') [7 8 0]
Feb 19 19:09:39 karymshakov NetworkManager[1238]: <info> Policy set 'System eth0
' (eth0) as default for IPv4 routing and DNS.
Feb 19 19:09:39 karymshakov NetworkManager[1238]: <info> Activation (eth0) succe
ssful, device activated.
Feb 19 19:09:39 karymshakov NetworkManager[1238]: <info> Activation (eth0) Stage
5 of 5 (IP Configure Commit) complete.
[root@karymshakov Рабочий стол]#
```

Рис. 3.12: Просмотр системного лог-файла

Просмотрел файл `/var/log/http/access_log` (рис - @fig:022).

Выполнил команду `semanage port -a -t http_port_t -p tcp 81`. После этого прове-
рил список портов командой `semanage port -l | grep http_port_t` (рис - @fig:024).
Убедился, что порт 81 появился в списке.

```
[root@karymshakov httpd]# semanage port -a -t http_port_t -p tcp 81
bash: semanage: команда не найдена
[root@karymshakov httpd]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@karymshakov httpd]# semanage port -l | grep http_port_t
bash: semanage: команда не найдена
```

Рис. 3.13: Просмотр портов

Вернул контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html` с
помощью команды `chcon -t httpd_sys_content_t /var/www/html/test.html` (рис -
@fig:025). После этого попробовал получить доступ к файлу через веб-сервер,
введя в браузере адрес `http://127.0.0.1:81/test.html` (рис - @fig:026).

```
bash: semanage: команда не найдена
root@karymshakov httpd]# chcon -t httpd_sys_content_t /var/www/html/test.html
root@karymshakov httpd]# rm /var/www/html/test.html
```

Рис. 3.14: Возвращение исходного контекста

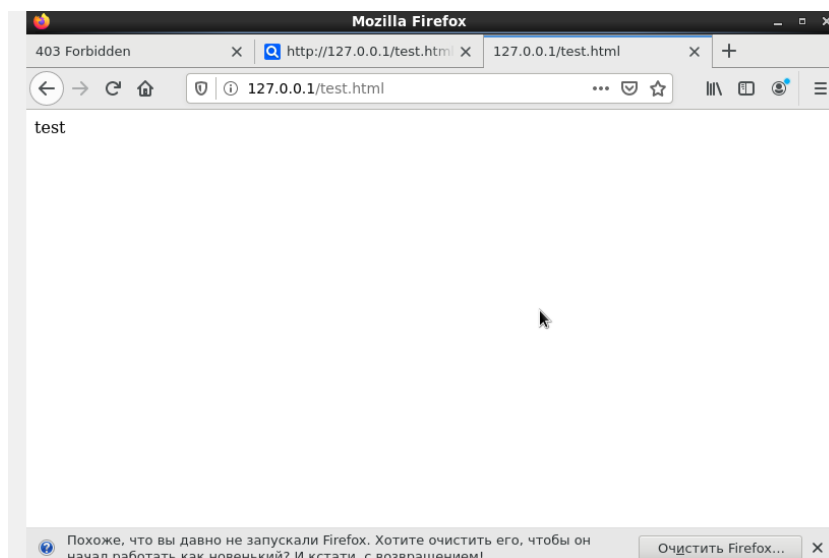


Рис. 3.15: Получение доступа к файлу через веб-сервер

Исправил обратно конфигурационный файл apache, вернув Listen 80 (рис - @fig:027).

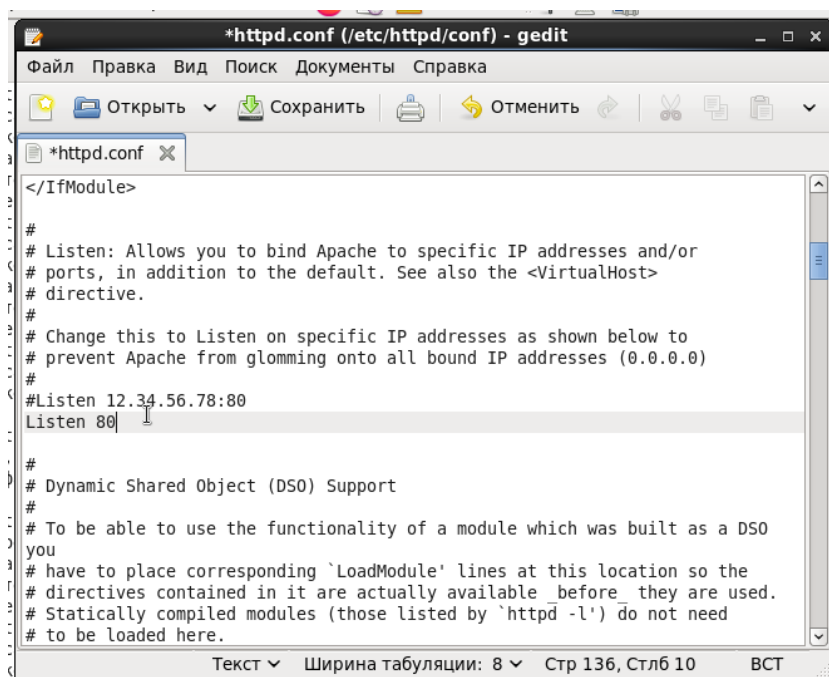
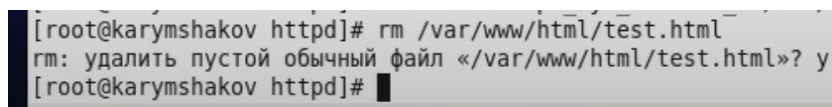


Рис. 3.16: Возвращение строки Listen 80

Удалил файл /var/www/html/test.html (рис - @fig:029).

A terminal window screenshot showing a root user at a machine named karymshakov. The user enters the command 'rm /var/www/html/test.html'. The terminal output shows the command being executed and a confirmation message in Russian: 'rm: удалить пустой обычный файл «/var/www/html/test.html»? y'. The prompt returns to the root user.

```
[root@karymshakov httpd]# rm /var/www/html/test.html
rm: удалить пустой обычный файл «/var/www/html/test.html»? y
[root@karymshakov httpd]#
```

Рис. 3.17: Удаление файла /var/www/html/test.html

4 Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux.

Проверил работу SELinx на практике совместно с веб-сервером Apache.

5 Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 6. Мандатное разграничение прав в Linux.