

Лабораторная работа №6

Мандатное разграничение прав в Linux

Дмитрий Константинович Федотов

Содержание

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

Список иллюстраций

3.1	Установка Apache	7
3.2	Внесение информации в конфигурационный файл	7
3.3	Отключение пакетного фильтра	8
3.4	Проверка режима работы SELinux	8
3.5	Проверка работы веб-сервера	8
3.6	Поиск веб-сервера Apache и определение его контекста безопасности	9
3.7	Текущее состояние переключателей SELinux для Apache	9
3.8	Статистика по политике	10
3.9	Определение типов файлов и поддиректорий, находящихся в директории /var/www	10
3.10	Определение типов файлов и поддиректорий, находящихся в директории /var/www/html	10
3.11	Пользователи, которым разрешено создание файлов в директории	11
3.12	html-файл и его содержимое	11
3.13	Контекст html-файл	11
3.14	Обращение к файлу через браузер	12
3.15	Выяснение контекста файла	12
3.16	Попытка получить доступ к файлу через веб-сервер	13
3.17	Изменение строки файла	13

Список таблиц

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. Подготовить лабораторный стенд и ознакомиться с методическими рекомендациями.
2. С помощью различных примеров ознакомиться с работой SELinux и веб-сервисом Apache.

3 Выполнение лабораторной работы

1. Подготовил лабораторный стенд и ознакомился с методическими рекомендациями.

Предварительно установил веб-сервис Apache с помощью команды `yum install httpd` (рис - @fig:001).

```
[dkfedotov@dkfedotov Рабочий стол]$ su
Пароль:
[root@dkfedotov Рабочий стол]# yum install httpd
Загружены модули: fastestmirror, refresh-packagekit, security
Подготовка к установке
Determining fastest mirrors
base | 3.7 kB | 00:00
extras | 3.3 kB | 00:00
updates | 3.4 kB | 00:00
Пакет httpd-2.2.15-69.el6.centos.i686 уже установлен, и это последняя версия.
Выполнять нечего
[root@dkfedotov Рабочий стол]#
```

Рис. 3.1: Установка Apache

В конфигурационном файле `/etc/httpd/httpd.conf` задал параметр `ServerName test.ru`. Это делается для того, чтобы при запуске веб-сервиса не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе (рис - @fig:002).

```
[root@dkfedotov httpd]# echo "ServerName test.ru" >> /etc/httpd/conf/httpd.conf
[root@dkfedotov httpd]# cat /etc/httpd/conf/httpd.conf
```

Рис. 3.2: Внесение информации в конфигурационный файл

Также отключил пакетный фильтр (рис - @fig:003).

```
[root@dkfedotov httpd]# cd ..
[root@dkfedotov etc]# cd httpd
[root@dkfedotov httpd]# iptables -F
[root@dkfedotov httpd]# iptables -p INPUT ACCEPT
iptables v1.4.7: unknown protocol 'input' specified
Try `iptables -h' or 'iptables --help' for more information.
[root@dkfedotov httpd]# iptables -P INPUT ACCEPT
[root@dkfedotov httpd]# iptables -P OUTPUT ACCEPT
[root@dkfedotov httpd]#
```

Рис. 3.3: Отключение пакетного фильтра

2. 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:004).

```
[root@dkfedotov httpd]# getenforce
Enforcing
[root@dkfedotov httpd]# sestatus
SELinux status:                enabled
SELinuxfs mount:              /selinux
Current mode:                  enforcing
Mode from config file:         enforcing
Policy version:                24
Policy from config file:       targeted
[root@dkfedotov httpd]#
```

Рис. 3.4: Проверка режима работы SELinux

Обратился 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:005).

```
Policy from config file:         targeted
[root@dkfedotov httpd]# service httpd status
httpd остановлен
[root@dkfedotov httpd]# /etc/rc.d/init.d/httpd status
httpd остановлен
[root@dkfedotov httpd]# /etc/rc.d/init.d/httpd start
Запускается httpd: [ OK ]
[root@dkfedotov httpd]# /etc/rc.d/init.d/httpd status
httpd (pid 2941) выполняется...
[root@dkfedotov httpd]#
```

Рис. 3.5: 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:006).

```
[root@dkfedotov httpd]# ps auxZ | grep httpd
unconfined_u:system_r:httpd_t:s0 root      2941  0.0  0.3 11644 3348 ?        S
s   17:58  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   2944  0.0  0.2 11644 2184 ?        S
   17:58  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   2945  0.0  0.2 11644 2184 ?        S
   17:58  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   2946  0.0  0.2 11644 2212 ?        S
   17:58  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   2947  0.0  0.2 11644 2184 ?        S
   17:58  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   2948  0.0  0.2 11644 2184 ?        S
   17:58  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   2949  0.0  0.2 11644 2184 ?        S
   17:58  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   2950  0.0  0.2 11644 2184 ?        S
   17:58  0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 apache   2951  0.0  0.2 11644 2184 ?        S
   17:58  0:00 /usr/sbin/httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 2961  0.0  0.0 4444 80
8 pts/0 S+ 17:59  0:00 grep httpd
[root@dkfedotov httpd]#
```

Рис. 3.6: Поиск веб-сервера Apache и определение его контекста безопасности

Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -b` (рис - @fig:007).

```
[root@dkfedotov httpd]# sestatus -b
SELinux status:                enabled
SELinuxfs mount:               /selinux
Current mode:                   enforcing
Mode from config file:         enforcing
Policy version:                 24
Policy from config file:       targeted

Policy booleans:
abrt_anon_write                 off
abrt_handle_event               off
allow_console_login             on
allow_cvs_read_shadow           off
allow_daemons_dump_core       on
allow_daemons_use_tcp_wrapper off
allow_daemons_use_tty         on
allow_domain_fd_use             on
allow_execheap                 off
allow_execmem                   on
allow_execmod                   on
```

Рис. 3.7: Текущее состояние переключателей SELinux для Apache

Посмотрел статистику по политике с помощью команды `seinfo`, а также определил множество пользователей, ролей, типов (рис - @fig:008).

```

[root@dkfedotov /]# cd /etc/httpd
[root@dkfedotov httpd]# seinfo

Statistics for policy file: /etc/selinux/targeted/policy/policy.24
Policy Version & Type: v.24 (binary, mls)

Classes:           81      Permissions:       238
Sensitivities:     1      Categories:       1024
Types:             3920    Attributes:        295
Users:             9      Roles:            12
Booleans:          237    Cond. Expr.:      277
Allow:             323336  Neverallow:        0
Auditallow:        141    Dontaudit:         274738
Type_trans:        42431  Type_change:       38
Type_member:        48    Role_allow:        19
Role_trans:        386    Range_trans:       6258
Constraints:        90    Validatetrans:     0
Initial SIDs:      27     Fs_use:            23
Genfscon:          84     Portcon:           474
Netifcon:           0     Nodecon:           0
Permissives:       90     Polcap:            2

[root@dkfedotov httpd]#

```

Рис. 3.8: Статистика по политике

Определил тип файлов и поддиректорий, находящихся в директории /var/www, с помощью команды `ls -lZ /var/www` (рис - @fig:009).

```

[root@dkfedotov httpd]# 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@dkfedotov httpd]#

```

Рис. 3.9: 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:010).

```

drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0
[root@dkfedotov httpd]# ls -lZ /var/www/html
[root@dkfedotov httpd]#

```

Рис. 3.10: Определение типов файлов и поддиректорий, находящихся в директории /var/www/html

Консоль ничего не выводит, поскольку директория пуста.

Определил круг пользователей, которым разрешено создание файлов в директории /var/www/html (рис - @fig:011).

```
[root@dkfedotov httpd]# ls -l /var/www
итого 16
drwxr-xr-x. 2 root root 4096 Июн 19 2018 cgi-bin
drwxr-xr-x. 3 root root 4096 Окт 16 01:01 error
drwxr-xr-x. 2 root root 4096 Июн 19 2018 html
drwxr-xr-x. 3 root root 4096 Окт 16 01:01 icons
[root@dkfedotov httpd]#
```

Рис. 3.11: Пользователи, которым разрешено создание файлов в директории

Создал от имени суперпользователя html-файл /var/www/html/test.html следующего содержания (рис - @fig:012):

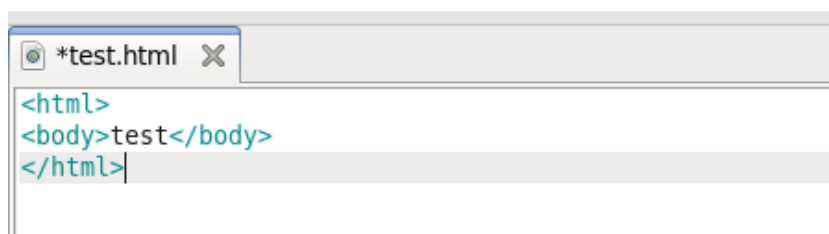


Рис. 3.12: html-файл и его содержимое

Проверил контекст созданного мною файла (рис - @fig:013):

```
[root@dkfedotov httpd]# 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@dkfedotov httpd]#
```

Рис. 3.13: Контекст html-файл

Обратился к файлу через веб-сервис, введя в браузере адрес `http://127.0.0.1/test.html` (рис - @fig:014):

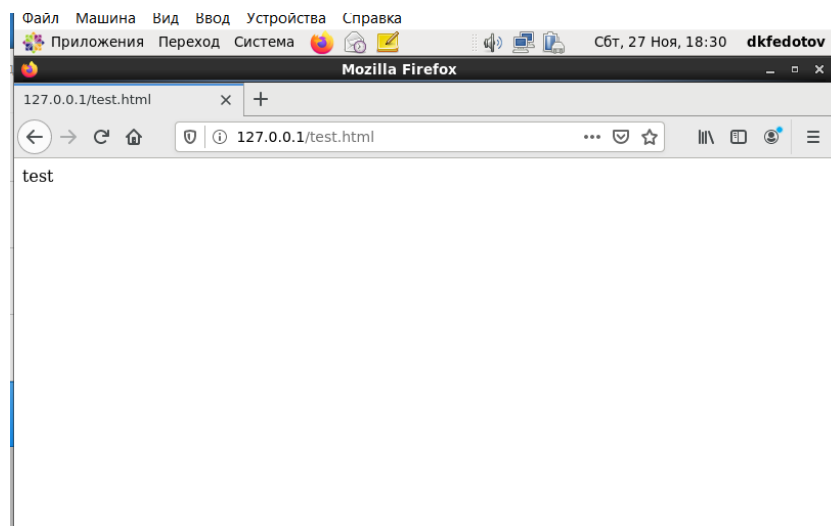


Рис. 3.14: Обращение к файлу через браузер

Проверил контекст файла с помощью команды `ls -Z /var/www/html/test.html` (рис - @fig:015).

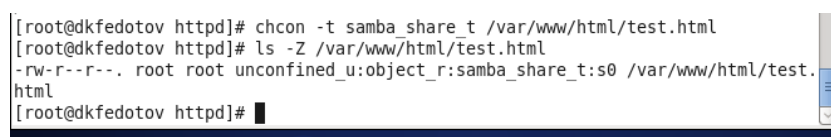


Рис. 3.15: Выяснение контекста файла

Изменил контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`.

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:016).

Forbidden

You don't have permission to access /test.html on this server.

Apache/2.2.15 (CentOS) Server at 127.0.0.1 Port 80

Рис. 3.16: 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`.

Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле `/etc/httpd/httpd.conf` нашел строчку `Listen 80` и заменил ее на `Listen 81` (рис - @fig:017).

```
#Listen 12.34.56.78:80
Listen 81
#
```

Рис. 3.17: Изменение строки файла

Просмотрел файл `/var/log/http/error_log`.

Просмотрел файл `/var/log/http/access_log`.

Просмотрел файл `var/log/audit/audit.log`.

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

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`. После этого попробовал получить доступ к файлу через веб-сервер, введя в браузере

адрес `http://127.0.0.1:81/test.html`.

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

Попытался удалить привязку `http_port_t` к 81 порту.

Удалил файл.

4 Выводы

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

Проверил работу SELinux 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.