

# **Отчет по лабораторной работе №6**

-

Овениязов Артур

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
4.1	ВАЖНО!!! Пунктов в отчете было бы необычайного много если отвечать скриншотом на каждый, поэтому многие пункты были объединены для более легкого составления отчета . . . . .	8
<b>5</b>	<b>Выводы</b>	<b>13</b>
	<b>Список литературы</b>	<b>14</b>

## Список иллюстраций

4.1	Результат выполнения 1-4 . . . . .	9
4.2	Результат выполнения 5-6 . . . . .	9
4.3	Результат выполнения 7-8 . . . . .	9
4.4	Результат выполнения 8-12 . . . . .	10
4.5	Результат выполнения 13-14 . . . . .	11
4.6	Результат выполнения 15 . . . . .	11
4.7	Результат выполнения 16 . . . . .	11
4.8	Результат выполнения 19 . . . . .	12
4.9	Результат выполнения 21-24 . . . . .	12

## 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 Задание

Лабораторная работа подразумевает практическое исследование дискреционных разграничений в современных системах с открытым кодом на базе ОС Linux, а именно изучение атрибутов для групп пользователей.

### 3 Теоретическое введение

SELinux (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена. Эти улучшения позволили SELinux стать универсальной системой, способной эффективно решать массу актуальных задач. Стоит помнить, что классическая система прав Unix применяется первой, и управление перейдет к SELinux только в том случае, если эта первичная проверка будет успешно пройдена. [1]

## 4 Выполнение лабораторной работы

### 4.1. ВАЖНО!!! Пунктов в отчете было бы необычайного много если отвечать скрином на каждый, поэтому многие пункты были объединены для более легкого составления отчета .

1-8. 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` или `/etc/rc.d/init.d/httpd status` Если не работает, запустите его так же, но с параметром `start`. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd` Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` Обратите внимание, что многие из них находятся в положении «off». Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www` 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`



```

aoveniyazov@aoveniyazov:/home/aoveniyazov
Файл Правка Вид Поиск Терминал Справка
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
Max kernel policy version: 31
[root@aoveniyazov aoveniyazov]# 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; vendor preset: disabled)
   Active: active (running) since Вт 2021-11-23 23:13:25 MSK; 5min ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 3450 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"
     Tasks: 6
    CGroup: /system.slice/httpd.service
            └─3450 /usr/sbin/httpd -DFOREGROUND
              └─3454 /usr/sbin/httpd -DFOREGROUND
                └─3455 /usr/sbin/httpd -DFOREGROUND
                  └─3456 /usr/sbin/httpd -DFOREGROUND
                    └─3457 /usr/sbin/httpd -DFOREGROUND
                      └─3458 /usr/sbin/httpd -DFOREGROUND

```

Рис. 4.1: Результат выполнения 1-4

```

[root@aoveniyazov aoveniyazov]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 3450 0.0 0.1 230440 5204 ? Ss 23:13 0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3454 0.0 0.0 232524 3152 ? S 23:13 0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3455 0.0 0.0 232524 3152 ? S 23:13 0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3456 0.0 0.0 232524 3152 ? S 23:13 0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3457 0.0 0.0 232524 3152 ? S 23:13 0:0
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3458 0.0 0.0 232524 3152 ? S 23:13 0:0
0 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3928 0.0 0.0 112032 968 pts/0 S+ 23
:19 0:00 grep --color=auto httpd
[root@aoveniyazov aoveniyazov]# sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]
  -v Verbose check of process and file contexts.
  -b Display current state of booleans.

```

Рис. 4.2: Результат выполнения 5-6

```

aoveniyazov@aoveniyazov:/home/aoveniyazov
Файл Правка Вид Поиск Терминал Справка
xdm_sysadm_login off
xdm_write_home off
xen_use_nfs off
xend_run_blktp on
xend_run_qemu on
xguest_connect_network on
xguest_exec_content on
xguest_mount_media on
xguest_use_bluetooth on
xserver_clients_write_xshm off
xserver_execmem off
xserver_object_manager off
zabbix_can_network off
zabbix_run_sudo off
zarafa_setrlimit off
zebra_write_config off
zoneminder_anon_write off
zoneminder_run_sudo off
[root@aoveniyazov aoveniyazov]# 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 html
[root@aoveniyazov aoveniyazov]# ls -lZ /var/www/html
[root@aoveniyazov aoveniyazov]# ls -lZ /var/www/html
[root@aoveniyazov aoveniyazov]# ls -lZ /var/www/html

```

Рис. 4.3: Результат выполнения 7-8

8-12. Создайте 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

Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html. Обратитесь к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедитесь, что файл был успешно отображён. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z. ls -Z /var/www/html/test.html`

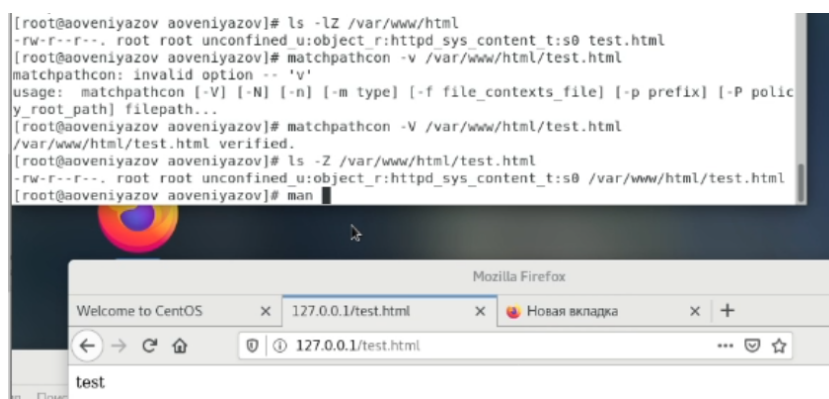


Рис. 4.4: Результат выполнения 8-12

13-24. 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` После этого проверьте, что контекст поменялся. 14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Вы должны получить сообщение об ошибке: `Forbidden You don't have permission to access /test.html on this server.`

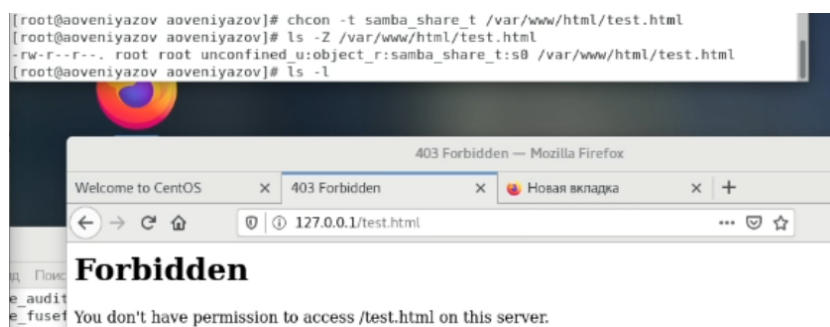


Рис. 4.5: Результат выполнения 13-14

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`.

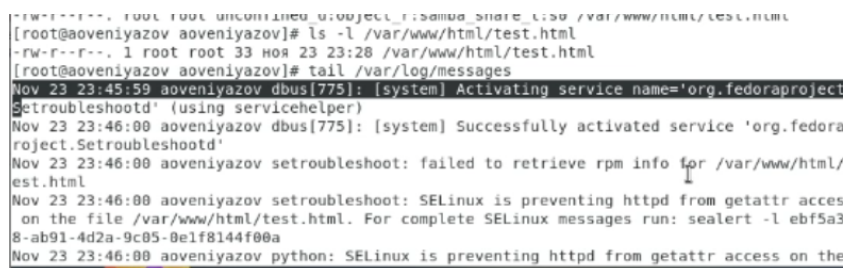


Рис. 4.6: Результат выполнения 15

16. Попробуйте 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`.

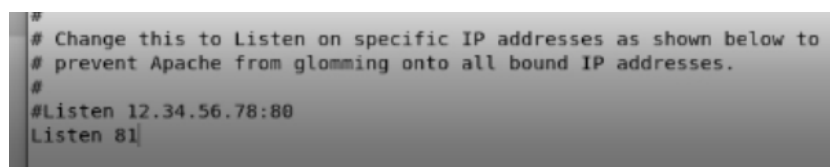


Рис. 4.7: Результат выполнения 16

19. 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.

```
[root@aoveniyazov aoveniyazov]# semanage port -a -t http_port_t -port tcp 81
usage: semanage [-h]
                {import,export,login,user,port,lbkey,lbendport,interface,module,node,fcontext,
boolean,permissive,dontaudit}
...
semanage: error: unrecognized arguments: 81
[root@aoveniyazov aoveniyazov]# 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@aoveniyazov aoveniyazov]#
```

Рис. 4.8: Результат выполнения 19

21. Верните контекст `httpd_sys_content_t` к файлу `/var/www/html/ test.html`:  
`chcon -t httpd_sys_content_t /var/www/html/test.html`
22. Исправьте обратно конфигурационный файл `apache`, вернув `Listen 80`.
23. Удалите привязку `http_port_t` к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.
24. Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html`

```
[root@aoveniyazov aoveniyazov]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@aoveniyazov aoveniyazov]# 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@aoveniyazov aoveniyazov]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@aoveniyazov aoveniyazov]#
```

Рис. 4.9: Результат выполнения 21-24

## 5 Выводы

Сегодня я приобрел практические навыки работы в консоли с атрибутами файлов, закрепил теоретические основы дискреционного разграничения доступа в соевытым кодом на базе ОС Linux и проверил работу SELinux на практике совместно с веб-сервером Apache

## Список литературы

1. Дискреционное разграничение доступа Linux [Электронный ресурс]. Сайт, 2021. URL: <http://debianinstall.ru/diskrektionnoe-razgranichenie-dostupa-linux/>.