

# **Лабораторная работа №6**

**Основы информационной безопасности**

Колчева Юлия Вячеславовна

# Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	12
4	Список литературы	13

# List of Figures

2.1	Ввод команд . . . . .	6
2.2	Обращение к веб-серверу . . . . .	6
2.3	Контекст безопасности . . . . .	7
2.4	Состояние . . . . .	7
2.5	Просмотр . . . . .	8
2.6	Создание и написание . . . . .	8
2.7	Обращение . . . . .	8
2.8	Просмотр . . . . .	8
2.9	Ошибка . . . . .	9
2.10	Работа с консолью . . . . .	9
2.11	Замена строки . . . . .	9
2.12	Перезапуск . . . . .	10
2.13	Содержание файла . . . . .	10
2.14	Работа с консолью . . . . .	10
2.15	Возвращение . . . . .	11
2.16	Содержимое файла . . . . .	11
2.17	Попытка удаления . . . . .	11
2.18	Удаление файла . . . . .	11

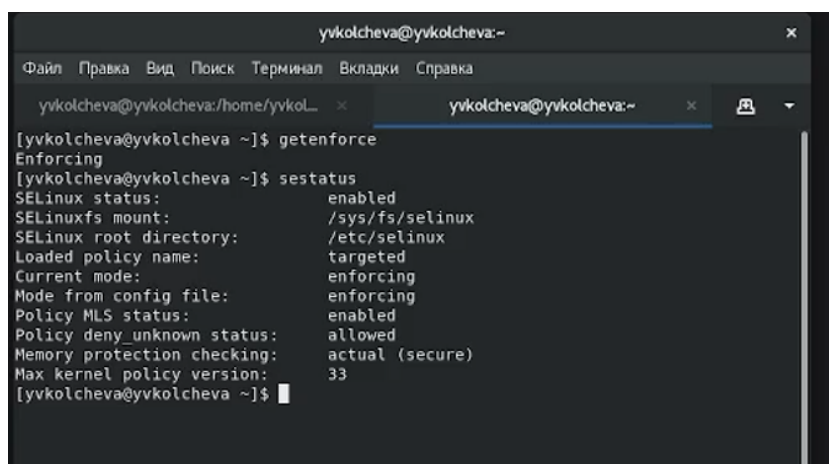
## List of Tables

# 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

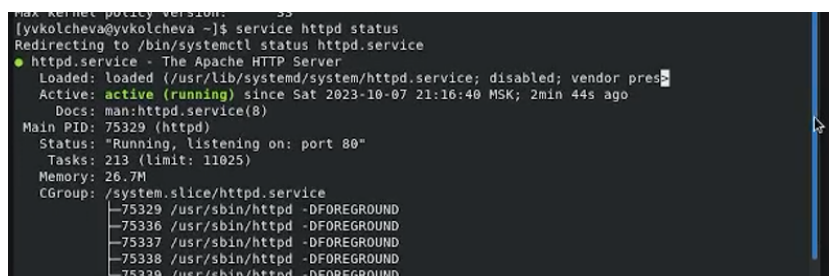
Вошла в систему под своей учетной записью и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд “getenforce” и “sestatus”(рис. 2.1)

A terminal window titled 'yvkolcheva@yvkolcheva:~' with a menu bar (Файл, Правка, Вид, Поиск, Терминал, Вкладки, Справка). The terminal shows the execution of 'getenforce' and 'sestatus' commands. The output of 'sestatus' shows SELinux is enabled, in enforcing mode, with the targeted policy loaded.

```
yvkolcheva@yvkolcheva:~$ getenforce
Enforcing
[yvkolcheva@yvkolcheva ~]$ 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
[yvkolcheva@yvkolcheva ~]$
```

Figure 2.1: Ввод команд

Обратилась с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает с помощью команды “service httpd status” (рис. 2.2)

A terminal window showing the output of the 'service httpd status' command. It indicates that the httpd service is active and running, with details about its loaded state, active status, and running processes.

```
[yvkolcheva@yvkolcheva ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: enabled)
   Active: active (running) since Sat 2023-10-07 21:16:40 MSK; 2min 44s ago
     Docs: man:httpd.service(8)
   Main PID: 75329 (httpd)
    Status: "Running, listening on: port 80"
     Tasks: 213 (limit: 11025)
    Memory: 26.7M
    CGroup: /system.slice/httpd.service
            └─75329 /usr/sbin/httpd -DFOREGROUND
              └─75336 /usr/sbin/httpd -DFOREGROUND
                └─75337 /usr/sbin/httpd -DFOREGROUND
                  └─75338 /usr/sbin/httpd -DFOREGROUND
                    └─75339 /usr/sbin/httpd -DFOREGROUND
```

Figure 2.2: Обращение к веб-серверу

С помощью команды “ps auxZ | grep httpd” определила контекст безопасности веб-сервера Apache - httpd\_t (рис. 2.3)

```

[yvkolcheva@yvkolcheva /home/yvkolcheva]
[yvkolcheva@yvkolcheva ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 75329 0.0 0.6 265100 11612 ? Ss 21:16 0:00 /usr/sbin/httpd
-DFOREGROUND
system_u:system_r:httpd_t:s0 apache 75336 0.0 0.4 269800 8704 ? S 21:16 0:00 /usr/sbin/httpd
-DFOREGROUND
system_u:system_r:httpd_t:s0 apache 75337 0.0 0.7 1458720 14356 ? Sl 21:16 0:00 /usr/sbin/httpd
-DFOREGROUND
system_u:system_r:httpd_t:s0 apache 75338 0.0 0.6 1327592 12304 ? Sl 21:16 0:00 /usr/sbin/httpd
-DFOREGROUND
system_u:system_r:httpd_t:s0 apache 75339 0.0 0.6 1327592 12304 ? Sl 21:16 0:00 /usr/sbin/httpd
-DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 yvkolcheva 75780 0.0 0.0 221940 1112 pts/1 R+ 21:22 0:00 gr
ep --color=auto httpd
[yvkolcheva@yvkolcheva ~]$ sestatus

```

Figure 2.3: Контекст безопасности

Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды “sestatus -bigrep httpd”. Посмотрела статистику по политике с помощью команды “seinfo”. Множество пользователей - 8, ролей - 14, типов 4995 (рис. 2.4)

```

Ibendportcon: 0 Ibkeycon: 0
Initial SIDs: 27 Fs_use: 34
Genfscon: 107 Portcon: 649
Netifcon: 0 Nodecon: 0

[yvkolcheva@yvkolcheva ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version: 31 (MLS enabled)
Target Policy: selinux
Handle unknown classes: allow
Classes: 132 Permissions: 464
Sensitivities: 1 Categories: 1024
Types: 5010 Attributes: 257
Users: 8 Roles: 14
Booleans: 342 Cond. Expr.: 390
Allow: 115052 Neverallow: 0
Auditallow: 168 Dontaudit: 10439
Type trans: 257620 Type change: 87
Type member: 35 Range trans: 5989
Role allow: 38 Role trans: 422
Constraints: 72 Validatetrans: 0
MLS Constrain: 72 MLS Val. Tran: 0
Permissives: 0 Polcap: 5
Defaults: 7 Typebounds: 0
Allowxperm: 0 Neverallowxperm: 0
Auditallowxperm: 0 Dontauditxperm: 0
Ibendportcon: 0 Ibkeycon: 0
Initial SIDs: 27 Fs_use: 34
Genfscon: 107 Portcon: 649
Netifcon: 0 Nodecon: 0
[yvkolcheva@yvkolcheva ~]$

```

Figure 2.4: Состояние

С помощью команды “ls -lZ /var/www” посмотрела файлы и поддиректории, находящиеся в директории /var/www. Используя команду “ls -lZ /var/www/html”, определила, что в данной директории файлов нет. Только владелец/суперпользователь может создавать файлы в директории /var/www/html (рис. 2.5)

```
Without options, show SELinux status.
[yvkolcheva@yvkolcheva ~]$ ls -lZ /var/www
итого 8
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 4096 сен 23 02:22 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 4096 сен 23 02:22 html
```

Figure 2.5: Просмотр

От имени суперпользователя создала html-файл /var/www/html/test.html. Контекст созданного файла - httpd\_sys\_content\_t (рис. 2.7)

```
[root@yvkolcheva yvkolcheva]# touch /var/www/html/test.html
[root@yvkolcheva yvkolcheva]# nano /var/www/html/test.html
[root@yvkolcheva yvkolcheva]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[root@yvkolcheva yvkolcheva]# su
[root@yvkolcheva yvkolcheva]# changeme
bash: changeme: команда не найдена...
[root@yvkolcheva yvkolcheva]# ls
AA Desktop Documents Downloads EXAMPLE Music Pictures Public Templates Videos
[root@yvkolcheva yvkolcheva]# ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 окт 7 21:32 test.html
[root@yvkolcheva yvkolcheva]#
```

Figure 2.6: Создание и написание

Обратилась к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”. Файл был успешно отображен (рис. 2.8)



Figure 2.7: Обращение

Изучив справку `man httpd_selinux`, выяснила, что для `httpd` определены следующие контексты файлов: `httpd_sys_content_t`, `httpd_sys_script_exec_t`, `httpd_sys_script_ro_t`, `httpd_sys_script_rw_t`, `httpd_sys_script_ra_t`, `httpd_unconfined_script_exec_t`. Контекст моего файла - `httpd_sys_content_t` (в таком случае содержимое должно быть доступно для всех скриптов `httpd` и для самого демона). Изменила контекст файла на `samba_share_t` командой “`sudo chcon -t samba_share_t /var/www/html/test.html`” и проверила, что контекст поменялся (рис. 2.8)

```
[root@yvkolcheva yvkolcheva]# ls -lZ /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@yvkolcheva yvkolcheva]# chcon -t samba_share_t /var/www/html/test.html
[root@yvkolcheva yvkolcheva]# ls -lZ /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@yvkolcheva yvkolcheva]#
```

Figure 2.8: Просмотр



Попробовала еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html” и получила сообщение об ошибке (т.к. к установленному ранее контексту процесс httpd не имеет доступа) (рис. 2.9)



Figure 2.9: Ошибка

Командой “ls -l /var/www/html/test.html” убедилась, что читать данный файл может любой пользователь. Просмотрела системный лог-файл веб-сервера Apache командой “sudo tail /var/log/messages”, отображающий ошибки (рис. 2.10)

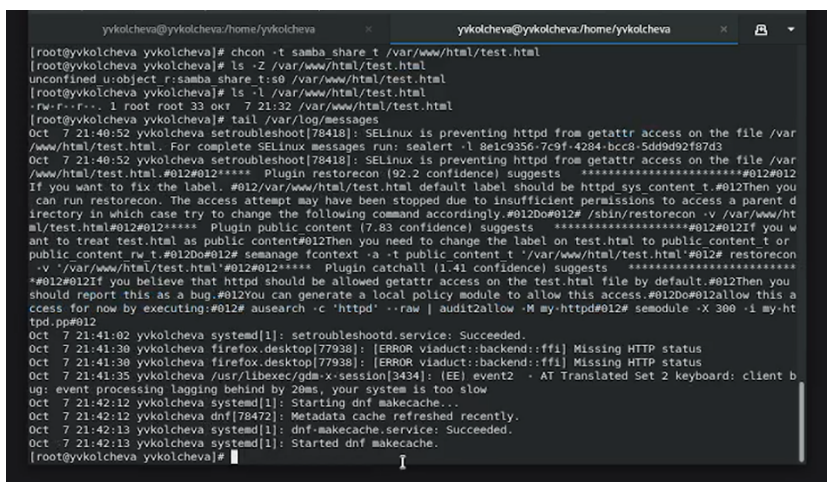


Figure 2.10: Работа с консолью

В файле /etc/httpd/conf/httpd.conf заменила строчку “Listen 80” на “Listen 81”, чтобы установить веб-сервер Apache на прослушивание TCP-порта 81 (рис. 2.11)

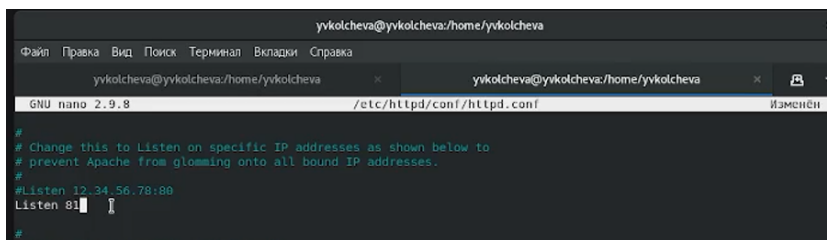


Figure 2.11: Замена строки

Перезапускаем веб-сервер Apache и анализируем лог-файлы командой “tail -nl /var/log/messages” 2.12)

```
[root@yvkolcheva yvkolcheva]# systemctl restart httpd
[root@yvkolcheva yvkolcheva]# tail -nl /var/log/messages
Oct 7 21:47:57 yvkolcheva httpd[78566]: Server configured, listening on: port 81
[root@yvkolcheva yvkolcheva]#
```

Figure 2.12: Перезапуск

Просмотрела файлы “var/log/http/error\_log”, “/var/log/http/access\_log” и “/var/log/audit/audit.log” и выяснила, что запись появилась в последнем файле (рис. 2.13)

```
yvkolcheva@yvkolcheva/home/yvkolcheva
r:httpd t:s0 key=(null) arch=x86_64 SYSCALL=stat AUDID="unset" UID="apache" GID="apache" EUID="apache" FSUID="apache"
EUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1696704041.002:334): proctitle=2F7573722F73626962F6874747064002D44464F524547524F554E44
type=AVC msg=audit(1696704041.003:335): avc: denied { getattr } for pid=75339 comm="httpd" path="/var/www/html/
test.html" dev="sdal" ino=1968374 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share
t:s0 tclass=file permssive=0
type=SYSCALL msg=audit(1696704041.003:335): arch=c0000003e syscall=6 success=no exit=-13 a0=7f5dce03deb8 a1=7f5dd36
ca890 a2=7f5dd36ca890 a3=1 items=0 ppid=75329 pid=75339 auid=4294967295 uid=48 gid=48 euid=48 fsuid=48 egl
d=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:
s0 key=(null) arch=x86_64 SYSCALL=stat AUDID="unset" UID="apache" GID="apache" EUID="apache" FSUID="apache"
EUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1696704041.003:335): proctitle=2F7573722F73626962F6874747064002D44464F524547524F554E44
type=SERVICE_START msg=audit(1696704045.432:336): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:
init_t:s0 msg=unit=setroubleshootd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? re
s=success AUDID="root" AUDID="unset"
type=SERVICE_STOP msg=audit(1696704062.985:337): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:
init_t:s0 msg=unit=setroubleshootd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? re
s=success AUDID="root" AUDID="unset"
type=SERVICE_START msg=audit(1696704133.101:338): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:
init_t:s0 msg=unit=dnf-makecache comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? re
s=success AUDID="root" AUDID="unset"
type=SERVICE_STOP msg=audit(1696704133.101:339): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:
init_t:s0 msg=unit=dnf-makecache comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? re
s=success AUDID="root" AUDID="unset"
type=SERVICE_START msg=audit(1696704477.582:341): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:
init_t:s0 msg=unit=httpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
AUDID="root" AUDID="unset"
type=SERVICE_STOP msg=audit(1696704477.582:341): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:
init_t:s0 msg=unit=httpd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
AUDID="root" AUDID="unset"
[root@yvkolcheva yvkolcheva]#
```

Figure 2.13: Содержание файла

Выполнила команду “semanage port -a -t http\_port\_t -p tcp 81” и убедилась, что порт TCP-81 установлен. Проверила список портов командой “semanage port -l | grep http\_port\_t”, убедилась, что порт 81 есть в списке и запускаем веб-сервер Apache снова (рис. 2.14)

```
[root@yvkolcheva yvkolcheva]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 уже определен
[root@yvkolcheva yvkolcheva]# 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@yvkolcheva yvkolcheva]# systemctl restart httpd
[root@yvkolcheva yvkolcheva]#
```

Figure 2.14: Работа с консолью

Вернула контекст “httpd\_sys\_content\_t” файлу “/var/www/html/test.html” командой “chcon -t httpd\_sys\_content\_t /var/www/html/test.html” (рис. 3.16) и по-

сле этого попробовала получить доступ к файлу через веб-сервер, введя адрес “http://127.0.0.1:81/test.html”, в результате чего увидела содержимое файла - слово “test” (рис. 2.15)(рис. 2.16)

```
pegasus_http_port_t tcp 5988
[root@yvkolcheva yvkolcheva]# systemctl restart httpd
[root@yvkolcheva yvkolcheva]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@yvkolcheva yvkolcheva]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@yvkolcheva yvkolcheva]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@yvkolcheva yvkolcheva]# nano /etc/httpd/conf/httpd.conf
[root@yvkolcheva yvkolcheva]#
```

Figure 2.15: Возвращение

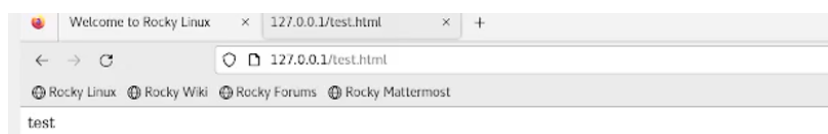


Figure 2.16: Содержимое файла

Исправила обратно конфигурационный файл apache, вернув “Listen 80”. Попыталась 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 (рис. 2.17)

```
[root@yvkolcheva yvkolcheva]# nano /etc/httpd/conf/httpd.conf
[root@yvkolcheva yvkolcheva]# semanage port -d -t http_port_t -p tcp 81\
>
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@yvkolcheva yvkolcheva]# semanage port -l | grep http_port_t
http_port_t      tcp      80, 81, 443, 488, 8088, 8089, 8443, 9000
pegasus_http_port_t tcp      5988
```

Figure 2.17: Попытка удаления

Удалила файл “/var/www/html/test.html” командой “rm /var/www/html/test.html” (рис. 2.17)

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

Figure 2.18: Удаление файла

## 3 Выводы

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

## 4 Список литературы

Лабораторная работа №6

SELinux – описание и особенности работы с системой [Электронный ресурс].  
URL: <https://habr.com/ru/company/kingservers/blog/209644/>.