

Лабораторная работа №6

Разважный Георгий НПИбд-02-19

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Выполнение лабораторной работы

1. Вошел в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted. Обратился с помощью браузера к веб-серверу, запущенному на компьютере, и убедился, что последний работает (рис. 1).

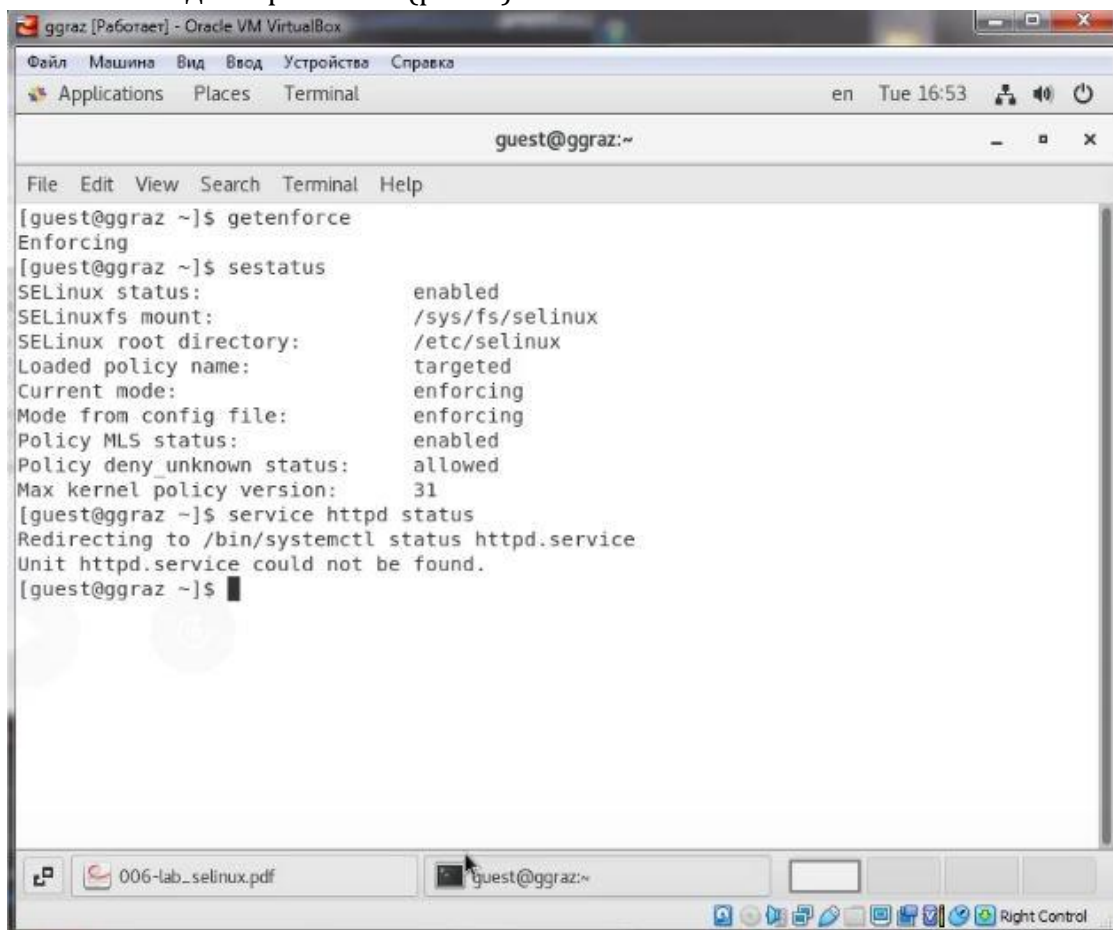


Рис. 1

2. Нашел веб-сервер Apache в списке процессов, определил его контекст безопасности (рис. 2).

The screenshot shows a terminal window titled "ggraz [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

```
File Edit View Search Terminal Help
● httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
  Active: inactive (dead)
  Docs: man:httpd(8)
       man:apachectl(8)
[guest@ggraz ~]$ ps auxZ | grep httpd
unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 guest 28121 0.0 0.0 112808 968 p
ts/1 R+ 16:59 0:00 grep --color=auto httpd
[guest@ggraz ~]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

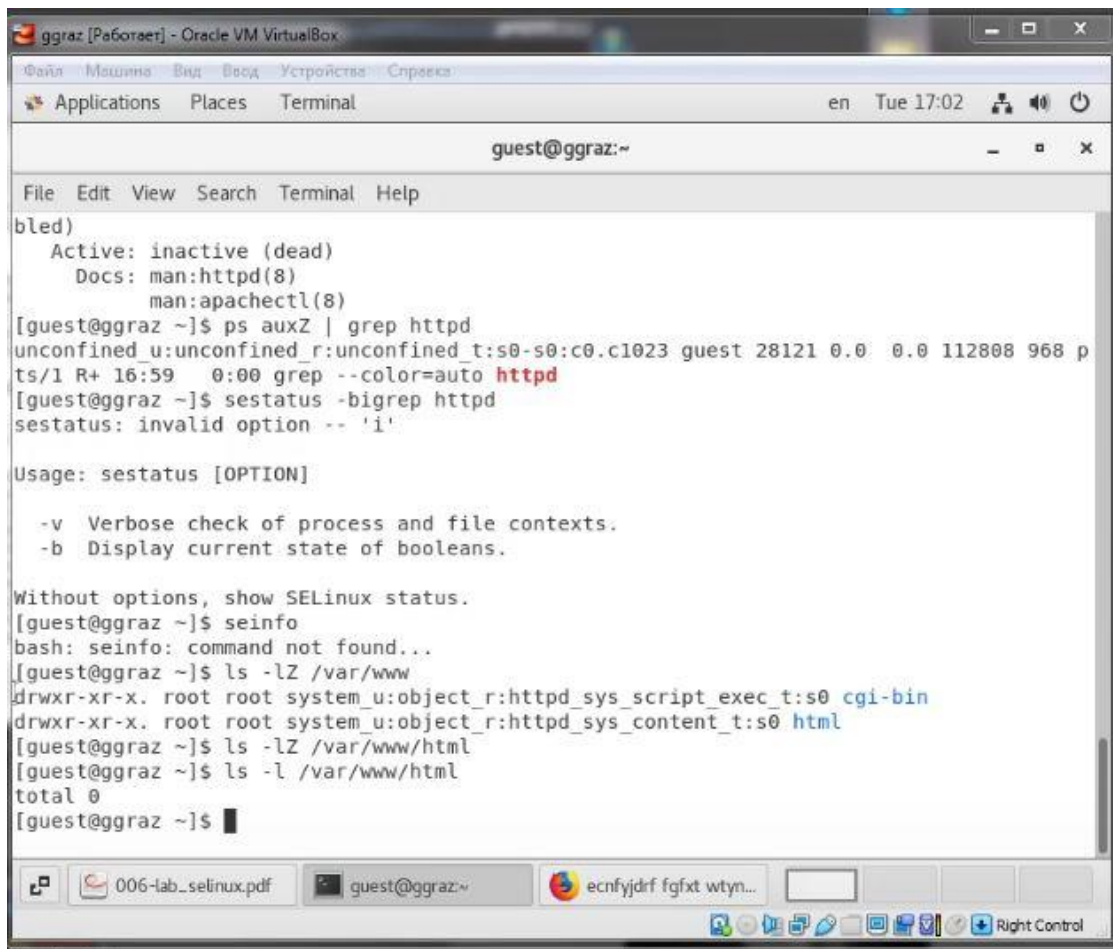
  -v Verbose check of process and file contexts.
  -b Display current state of booleans.

Without options, show SELinux status.
[guest@ggraz ~]$ seinfo
bash: seinfo: command not found...
[guest@ggraz ~]$ 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
[guest@ggraz ~]$ ls -lZ /var/www/html
[guest@ggraz ~]$
```

The terminal window also shows a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". The status bar at the bottom indicates "en Tue 17:01".

Рис. 2

3. Посмотрел текущее состояние переключателей SELinux для Apache (рис. 3).



```
ggraz [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Applications Places Terminal en Tue 17:02
guest@ggraz:~
File Edit View Search Terminal Help
bled)
  Active: inactive (dead)
  Docs: man:htpд(8)
       man:apachectl(8)
[guest@ggraz ~]$ ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 guest 28121 0.0  0.0 112808 968 p
ts/1 R+ 16:59  0:00 grep --color=auto httpd
[guest@ggraz ~]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

  -v Verbose check of process and file contexts.
  -b Display current state of booleans.

Without options, show SELinux status.
[guest@ggraz ~]$ seinfo
bash: seinfo: command not found...
[guest@ggraz ~]$ 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
[guest@ggraz ~]$ ls -lZ /var/www/html
[guest@ggraz ~]$ ls -l /var/www/html
total 0
[guest@ggraz ~]$
```

Рис. 3

4. Посмотрел статистику по политике с помощью команды `seinfo`, также определил множество пользователей, ролей, типов.
5. Определил тип файлов и поддиректорий, находящихся в директории `/var/www`. Определил тип файлов, находящихся в директории `/var/www/html`. Определил круг пользователей, которым разрешено создание файлов в директории (рис. 4).

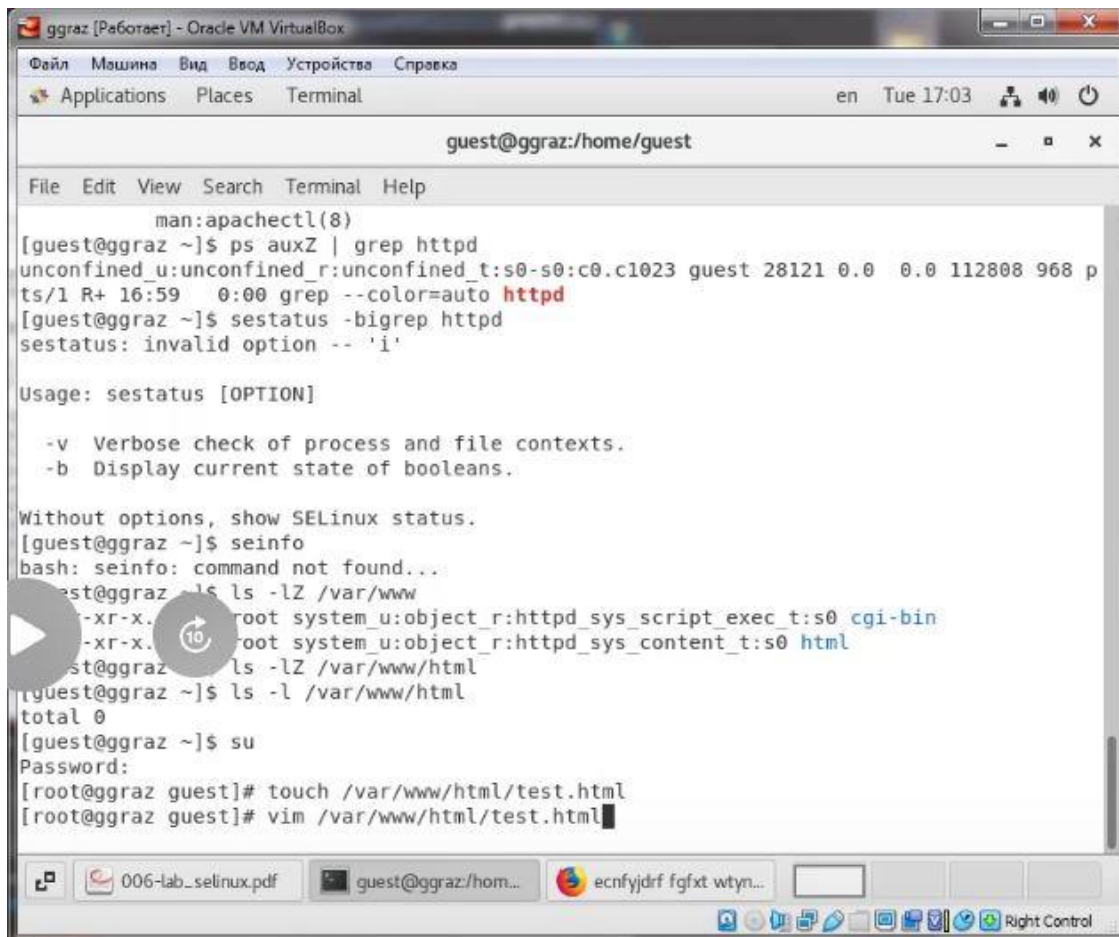


Рис. 4

6. Создал от имени суперпользователя html-файл (рис. 5).

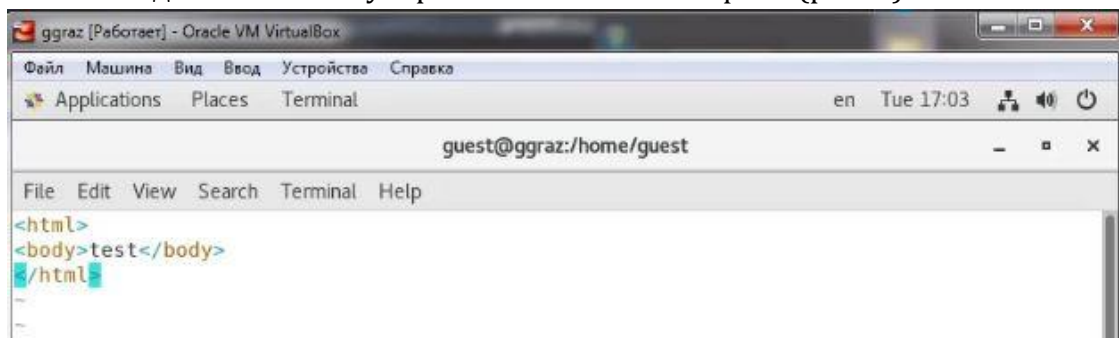
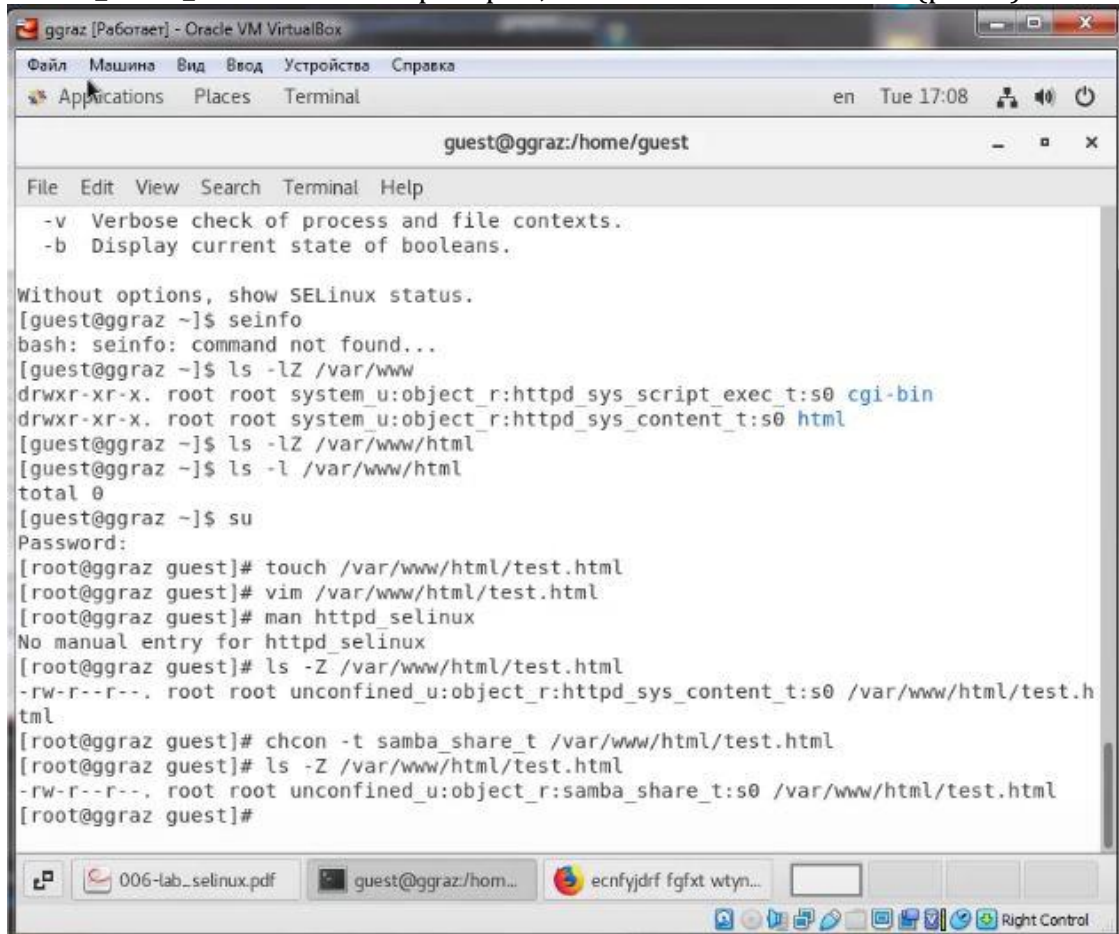


Рис. 5

7. Проверил контекст созданного файла. Контекст, присваиваемый по умолчанию вновь созданным файлам в директории `/var/www/html`: `httpd_sys_content` (рис. 6).
8. Обратился к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедился, что файл успешно отображён (рис. 7).

9. Изменил контекст файла /var/www/html/test.html с httpd_sys_content_t на samba_share_t. После этого проверил, что контекст поменялся (рис. 8).



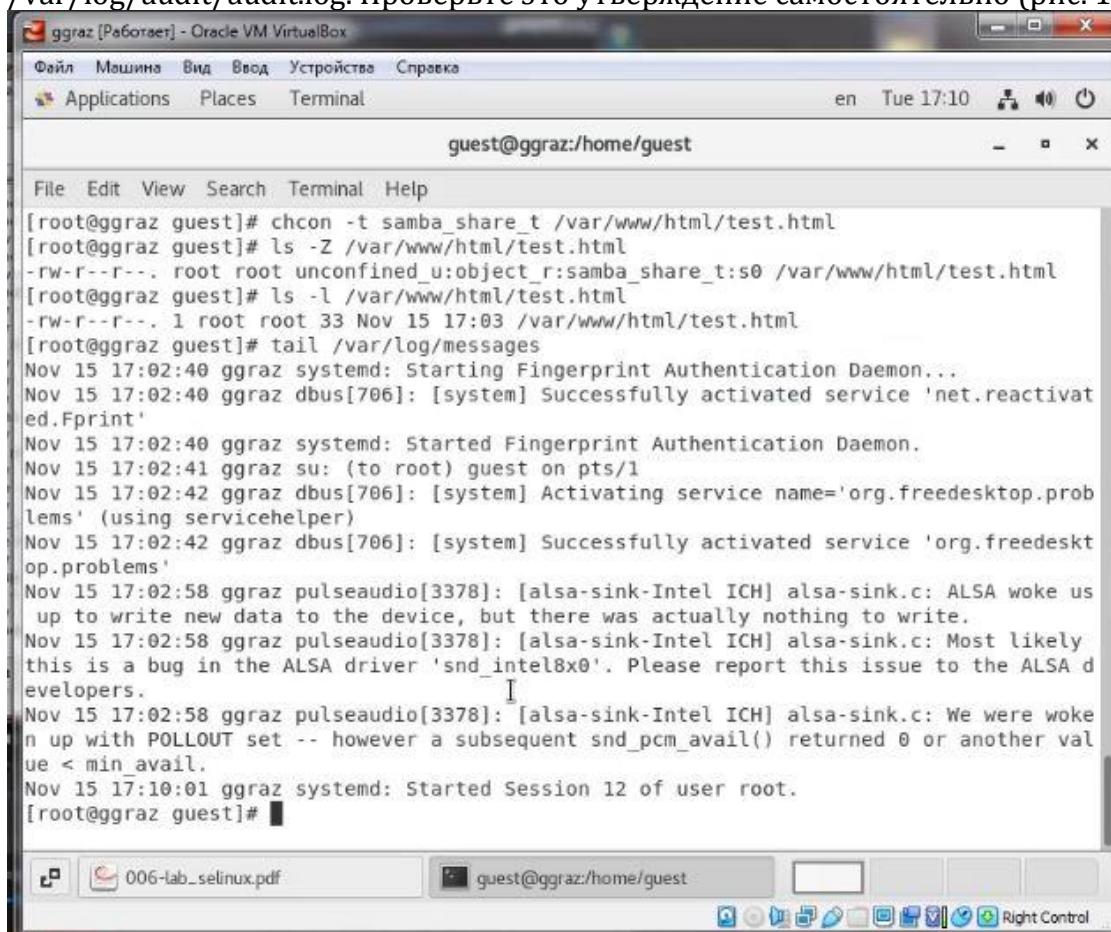
```
ggraz [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Places  Terminal
en  Tue 17:08
guest@ggraz:/home/guest

File Edit View Search Terminal Help
-v Verbose check of process and file contexts.
-b Display current state of booleans.

Without options, show SELinux status.
[guest@ggraz ~]$ seinfo
bash: seinfo: command not found...
[guest@ggraz ~]$ 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
[guest@ggraz ~]$ ls -lZ /var/www/html
[guest@ggraz ~]$ ls -l /var/www/html
total 0
[guest@ggraz ~]$ su
Password:
[root@ggraz guest]# touch /var/www/html/test.html
[root@ggraz guest]# vim /var/www/html/test.html
[root@ggraz guest]# man httpd_selinux
No manual entry for httpd_selinux
[root@ggraz guest]# 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@ggraz guest]# chcon -t samba_share_t /var/www/html/test.html
[root@ggraz guest]# 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
[root@ggraz guest]#
```

10. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html> (рис. 9).
11. Проанализировал ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? Просмотрел log-файлы веб-сервера Apache. Также просмотрите системный лог-файл. Если в системе окажутся запущенными процессы setroubleshootd и auditd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле

/var/log/audit/audit.log. Проверьте это утверждение самостоятельно (рис. 10).

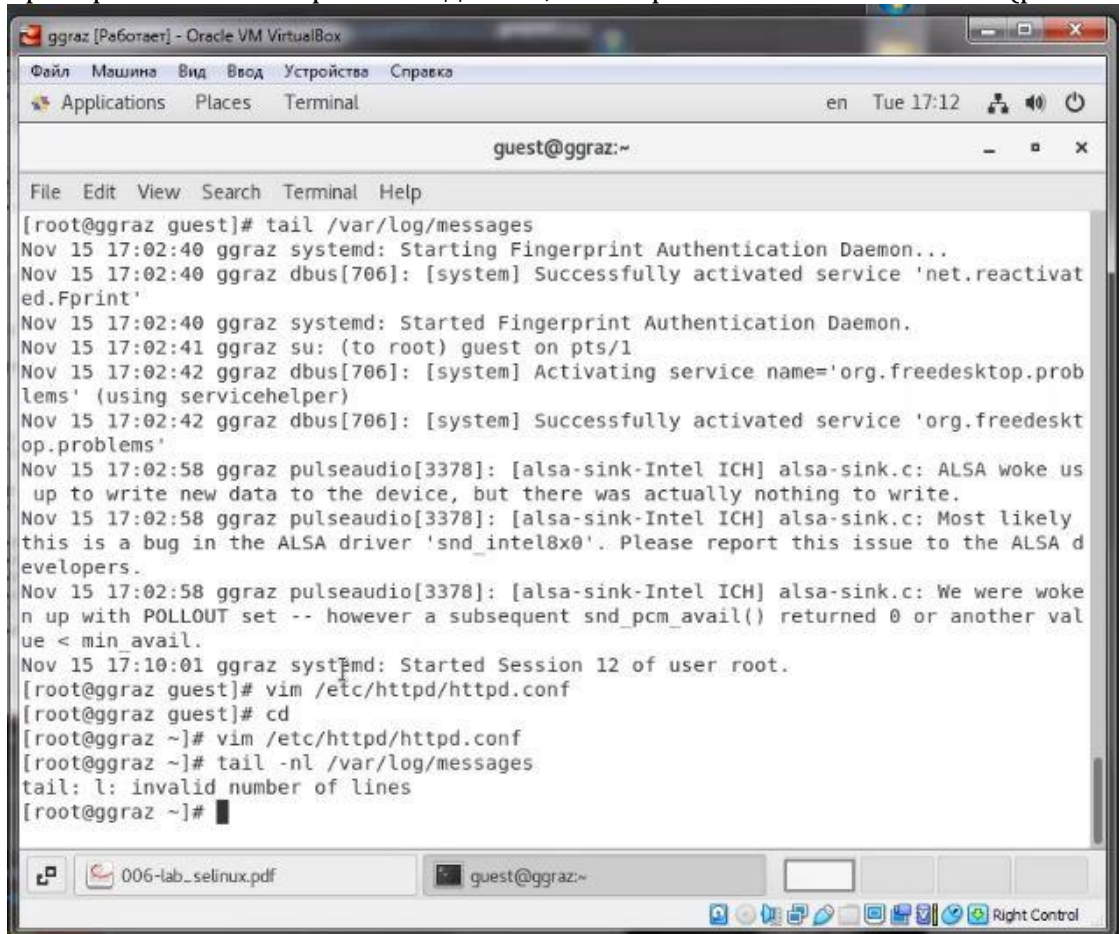


```
ggraz [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Places  Terminal
en  Tue 17:10
guest@ggraz:/home/guest

File Edit View Search Terminal Help
[root@ggraz guest]# chcon -t samba_share_t /var/www/html/test.html
[root@ggraz guest]# 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
[root@ggraz guest]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Nov 15 17:03 /var/www/html/test.html
[root@ggraz guest]# tail /var/log/messages
Nov 15 17:02:40 ggraz systemd: Starting Fingerprint Authentication Daemon...
Nov 15 17:02:40 ggraz dbus[706]: [system] Successfully activated service 'net.reactivated.Fprint'
Nov 15 17:02:40 ggraz systemd: Started Fingerprint Authentication Daemon.
Nov 15 17:02:41 ggraz su: (to root) guest on pts/1
Nov 15 17:02:42 ggraz dbus[706]: [system] Activating service name='org.freedesktop.problems' (using servicehelper)
Nov 15 17:02:42 ggraz dbus[706]: [system] Successfully activated service 'org.freedesktop.problems'
Nov 15 17:02:58 ggraz pulseaudio[3378]: [alsa-sink-Intel ICH] alsa-sink.c: ALSA woke us up to write new data to the device, but there was actually nothing to write.
Nov 15 17:02:58 ggraz pulseaudio[3378]: [alsa-sink-Intel ICH] alsa-sink.c: Most likely this is a bug in the ALSA driver 'snd_intel8x0'. Please report this issue to the ALSA developers.
Nov 15 17:02:58 ggraz pulseaudio[3378]: [alsa-sink-Intel ICH] alsa-sink.c: We were woken up with POLLOUT set -- however a subsequent snd_pcm_avail() returned 0 or another value < min avail.
Nov 15 17:10:01 ggraz systemd: Started Session 12 of user root.
[root@ggraz guest]#
```

12. Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле /etc/httpd/httpd.conf нашёл строчку Listen 80 и заменил её на Listen 81 (рис. 11).
13. Выполнил перезапуск веб-сервера Apache. (рис. 12).
14. Проанализировала лог-файлы. Просмотрела файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log (рис. 13).

15. Выполнила команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверила список портов. Убедилась, что порт 81 появился в списке (рис. 14).



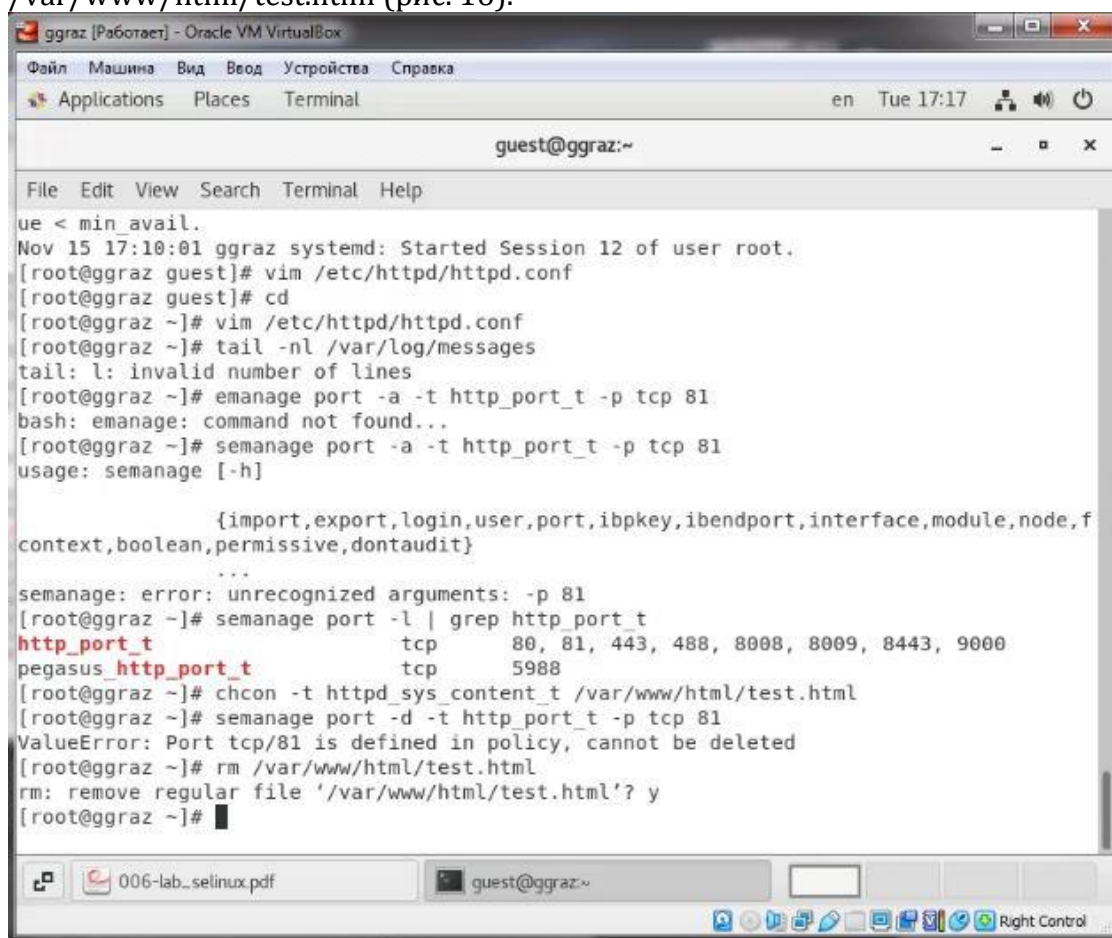
The screenshot shows a terminal window titled "ggraz [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar are tabs for "Applications", "Places", and "Terminal". The terminal content shows the following sequence of events:

```
guest@ggraz:~  
File Edit View Search Terminal Help  
[root@ggraz guest]# tail /var/log/messages  
Nov 15 17:02:40 ggraz systemd: Starting Fingerprint Authentication Daemon...  
Nov 15 17:02:40 ggraz dbus[706]: [system] Successfully activated service 'net.reactivat  
ed.Fprint'  
Nov 15 17:02:40 ggraz systemd: Started Fingerprint Authentication Daemon.  
Nov 15 17:02:41 ggraz su: (to root) guest on pts/1  
Nov 15 17:02:42 ggraz dbus[706]: [system] Activating service name='org.freedesktop.pro  
blems' (using servicehelper)  
Nov 15 17:02:42 ggraz dbus[706]: [system] Successfully activated service 'org.freedesk  
top.problems'  
Nov 15 17:02:58 ggraz pulseaudio[3378]: [alsa-sink-Intel ICH] alsa-sink.c: ALSA woke us  
up to write new data to the device, but there was actually nothing to write.  
Nov 15 17:02:58 ggraz pulseaudio[3378]: [alsa-sink-Intel ICH] alsa-sink.c: Most likely  
this is a bug in the ALSA driver 'snd_intel8x0'. Please report this issue to the ALSA d  
evelopers.  
Nov 15 17:02:58 ggraz pulseaudio[3378]: [alsa-sink-Intel ICH] alsa-sink.c: We were woken  
up with POLLOUT set -- however a subsequent snd_pcm_avail() returned 0 or another val  
ue < min_avail.  
Nov 15 17:10:01 ggraz systemd: Started Session 12 of user root.  
[root@ggraz guest]# vim /etc/httpd/httpd.conf  
[root@ggraz guest]# cd  
[root@ggraz ~]# vim /etc/httpd/httpd.conf  
[root@ggraz ~]# tail -nl /var/log/messages  
tail: l: invalid number of lines  
[root@ggraz ~]#
```

The bottom of the window shows a taskbar with icons for a window, a PDF file named "006-lab_selinux.pdf", and the terminal window itself. The system tray on the right includes a "Right Control" button.

16. Вернула контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html` (рис. 15).
17. Исправила обратно конфигурационный файл `apache`, вернув `Listen80`.

18. Удалила привязку `http_port_t` к 81 порту. Удалила файл `/var/www/html/test.html` (рис. 16).



The screenshot shows a terminal window titled "ggraz [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

```
ue < min_avail.
Nov 15 17:10:01 ggraz systemd: Started Session 12 of user root.
[root@ggraz guest]# vim /etc/httpd/httpd.conf
[root@ggraz guest]# cd
[root@ggraz ~]# vim /etc/httpd/httpd.conf
[root@ggraz ~]# tail -nl /var/log/messages
tail: l: invalid number of lines
[root@ggraz ~]# emanage port -a -t http_port_t -p tcp 81
bash: emanage: command not found...
[root@ggraz ~]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
                    {import,export,login,user,port,ibpkey,ibendport,interface,module,node,f
context,boolean,permissive,dontaudit}
...
semanage: error: unrecognized arguments: -p 81
[root@ggraz ~]# 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@ggraz ~]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@ggraz ~]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@ggraz ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@ggraz ~]#
```

Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.