

Лабораторная работа №6

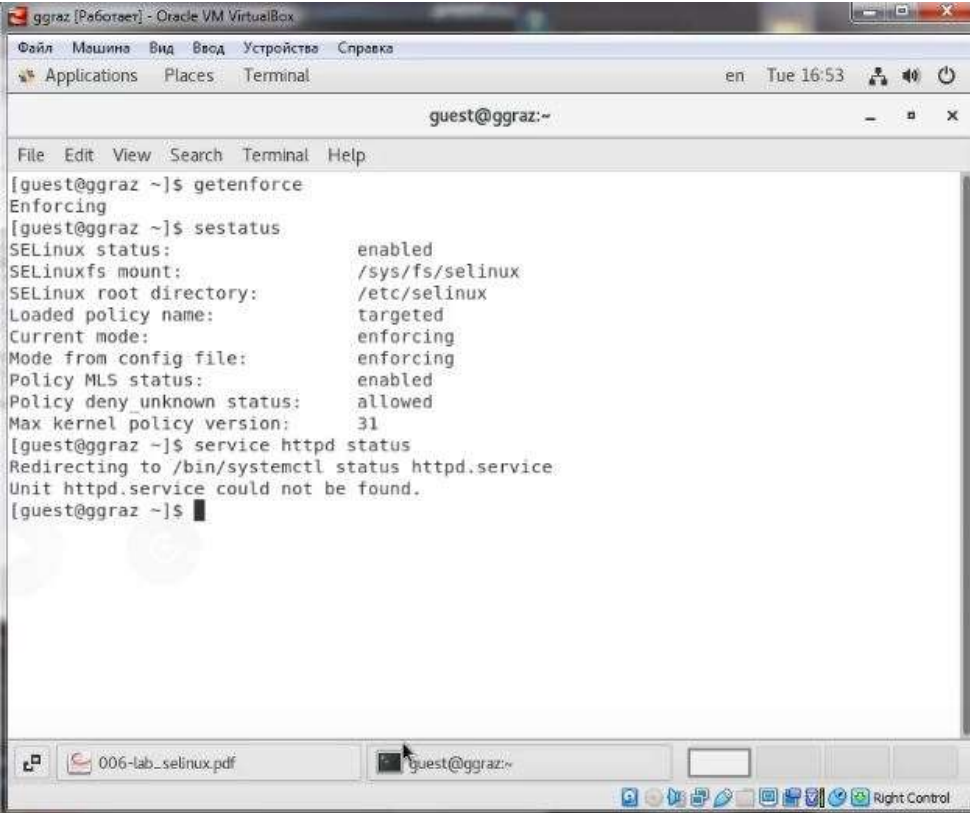
Разважный Георгий НПИбд-02-19

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).



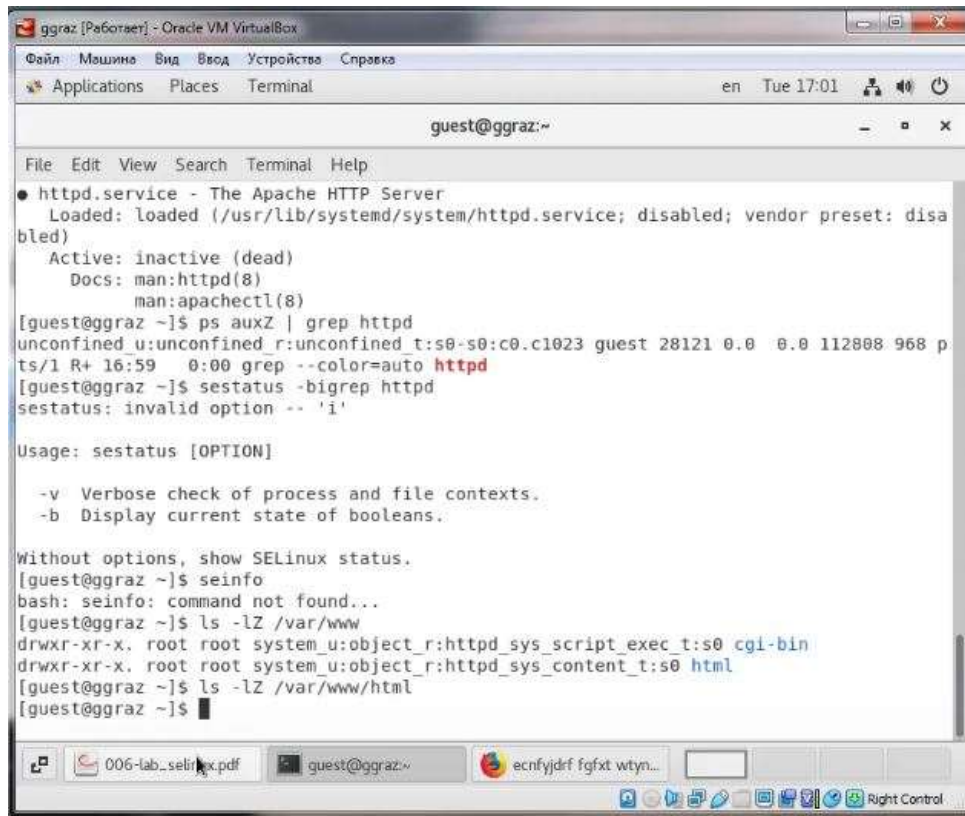
The screenshot shows a terminal window titled "ggraz [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройство", and "Справка". Below the menu bar is a toolbar with icons for Applications, Places, and Terminal. The terminal itself has a title bar "guest@ggraz:~" and a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal content shows the following commands and output:

```
[guest@ggraz ~]$ getenforce
Enforcing
[guest@ggraz ~]$ 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
Max kernel policy version:      31
[guest@ggraz ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
Unit httpd.service could not be found.
[guest@ggraz ~]$
```

At the bottom of the window, there is a taskbar with a file icon, a PDF icon labeled "006-lab_selinux.pdf", and a terminal icon labeled "guest@ggraz:~". On the far right of the taskbar is a "Right Control" button.

Рис. 1

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



```
ggraz [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Applications  Places  Terminal
en  Tue 17:01

guest@ggraz:~

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'

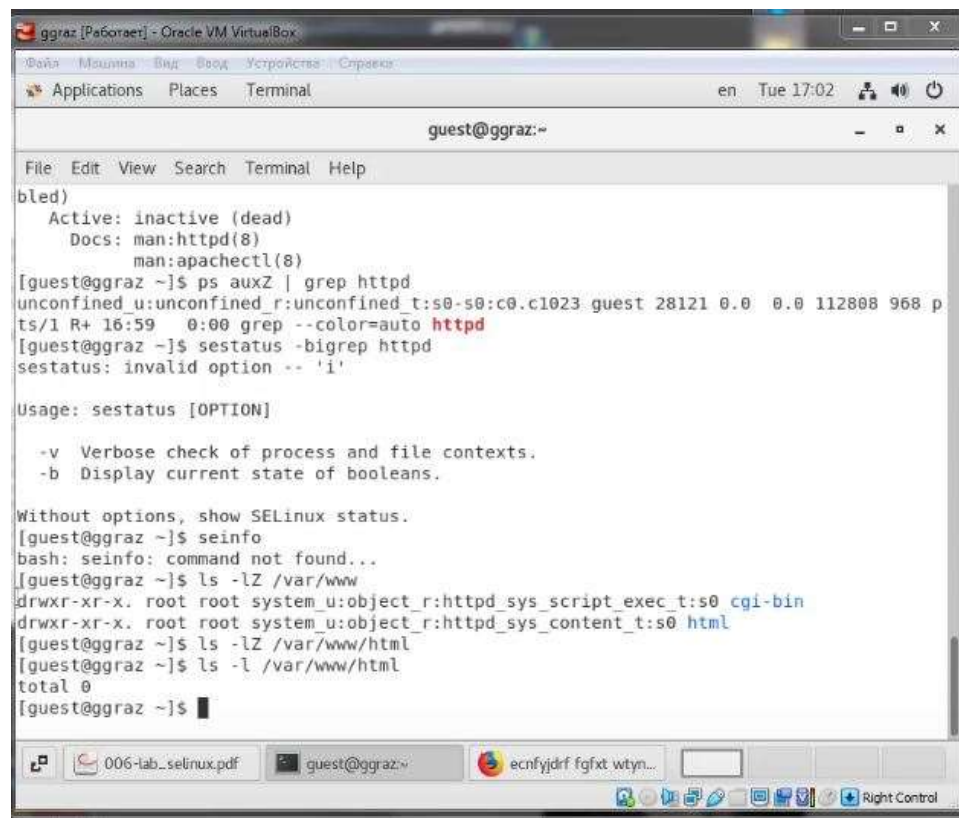
Usage: sestatus [OPTION]

  -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 ~]$
```

Рис. 2

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



```
ggraz [Рабочий] - Oracle VM VirtualBox
Applications Places Terminal en Tue 17:02
guest@ggraz:~
File Edit View Search Terminal Help
bled)
  Active: inactive (dead)
  Docs: man:htp(8)
       man:apachectl(8)
[guest@ggraz ~]$ ps auxZ | grep htp
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 htp
[guest@ggraz ~]$ sestatus -bigrep htp
sestatus: invalid option -- 'i'

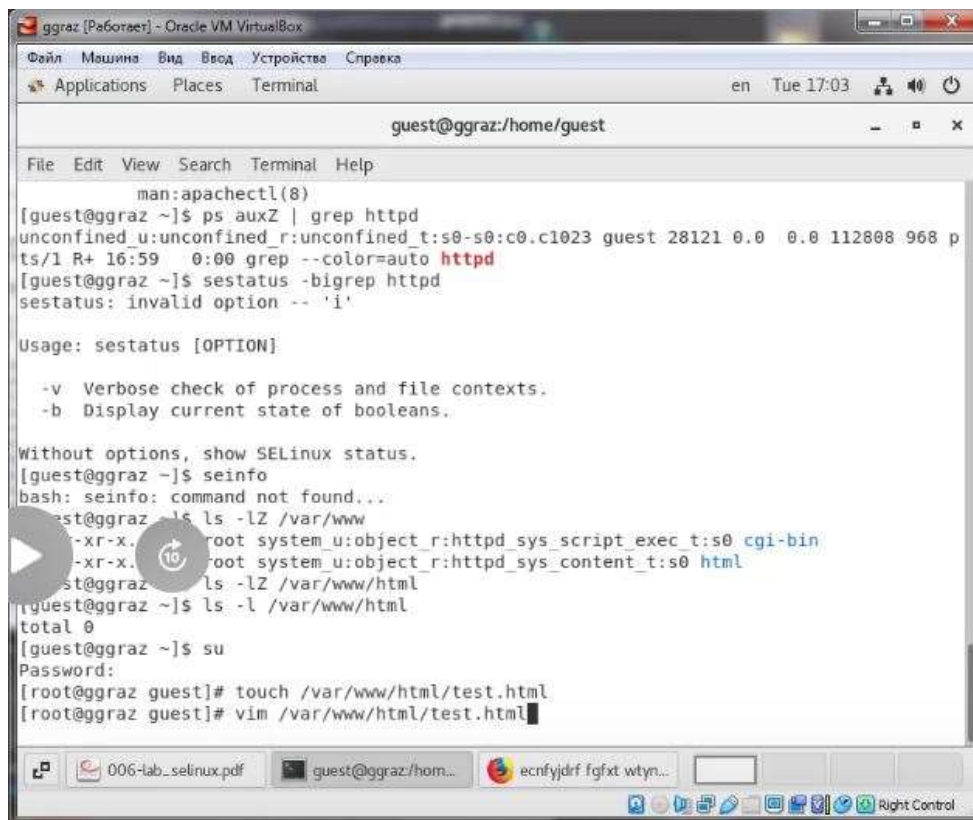
Usage: sestatus [OPTION]

  -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:htp_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:htp_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).



```
ggraz [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Вход  Устройство  Справка
Applications  Places  Terminal
en  Tue 17:03  [User Icon] [Volume Icon] [Power Icon]

guest@ggraz:/home/guest

File Edit View Search Terminal Help

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'

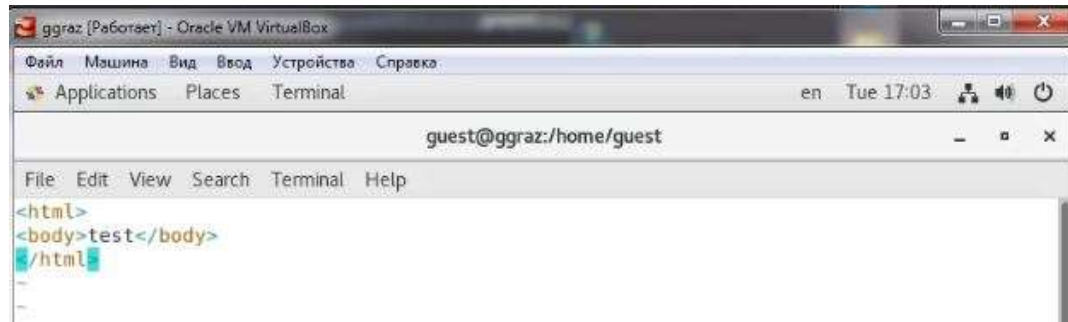
Usage: sestatus [OPTION]

  -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
-r-xr-x.  root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
-r-xr-x.  root system_u:object_r:httpd_sys_content_t:s0 html
[guest@ggraz ~]$ ls -lZ /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
```

Рис. 4

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



The image 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 is a toolbar with "Applications", "Places", and "Terminal". The status bar at the top right shows "en", "Tue 17:03", and system icons. The terminal prompt is "guest@ggraz:/home/guest". The terminal has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal content shows the following commands and output:

```
<html>
<body>test</body>
</html>
```

Рис. 5

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). Рис. 8

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 `audtd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно (рис. 10). Рис. 10

15.Выполнил команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверил список портов. Убедился, что порт 81 появился в списке (рис. 14). Рис. 14

17.Исправил обратно конфигурационный файл apache, вернув Listen80.

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

Выводы

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