

Лабораторная работа №6

Унтевская Валерия НПИбд-02-19

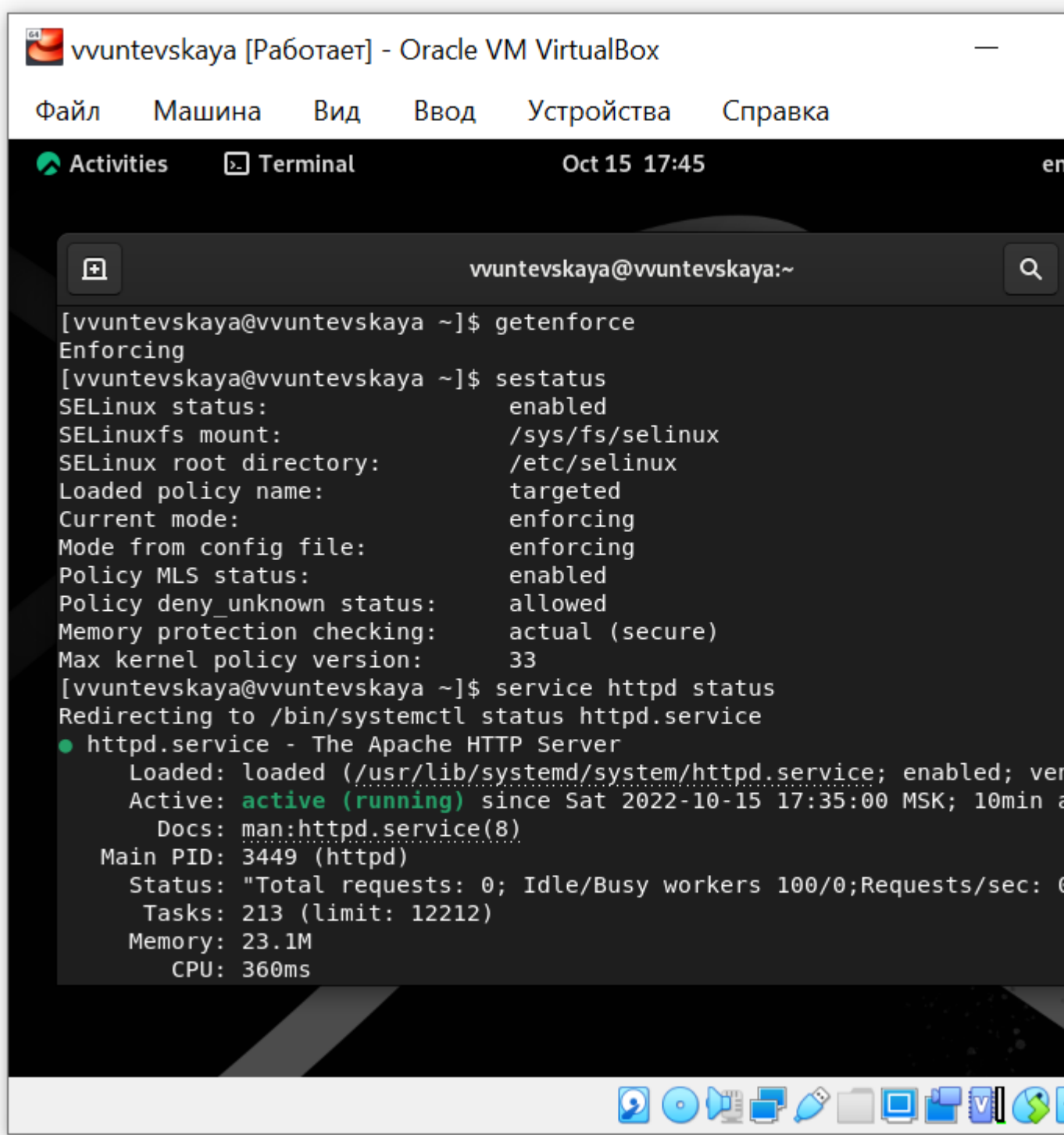
Цель работы

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. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в

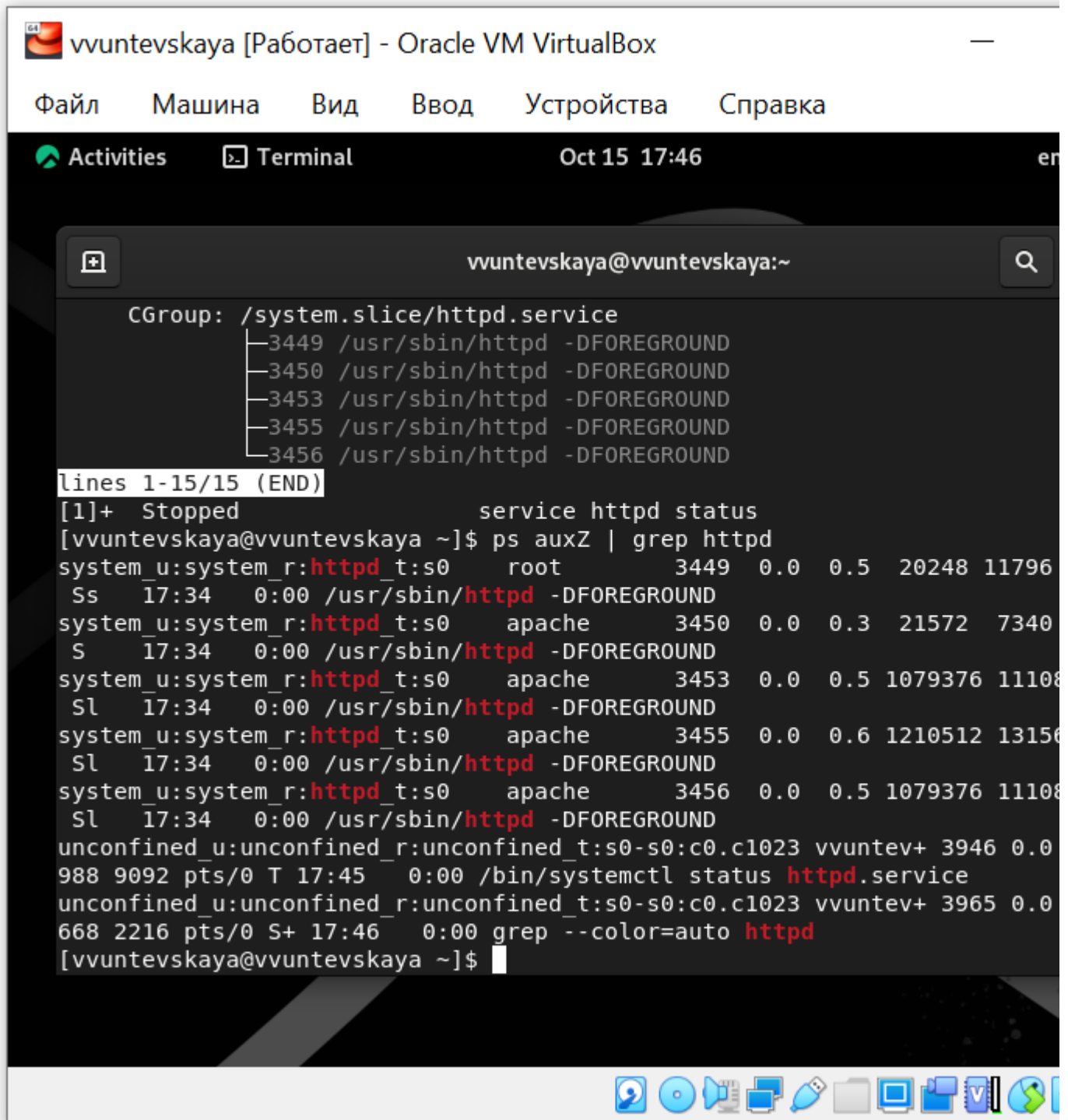
режиме enforcing политики targeted. Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает (рис. 1).



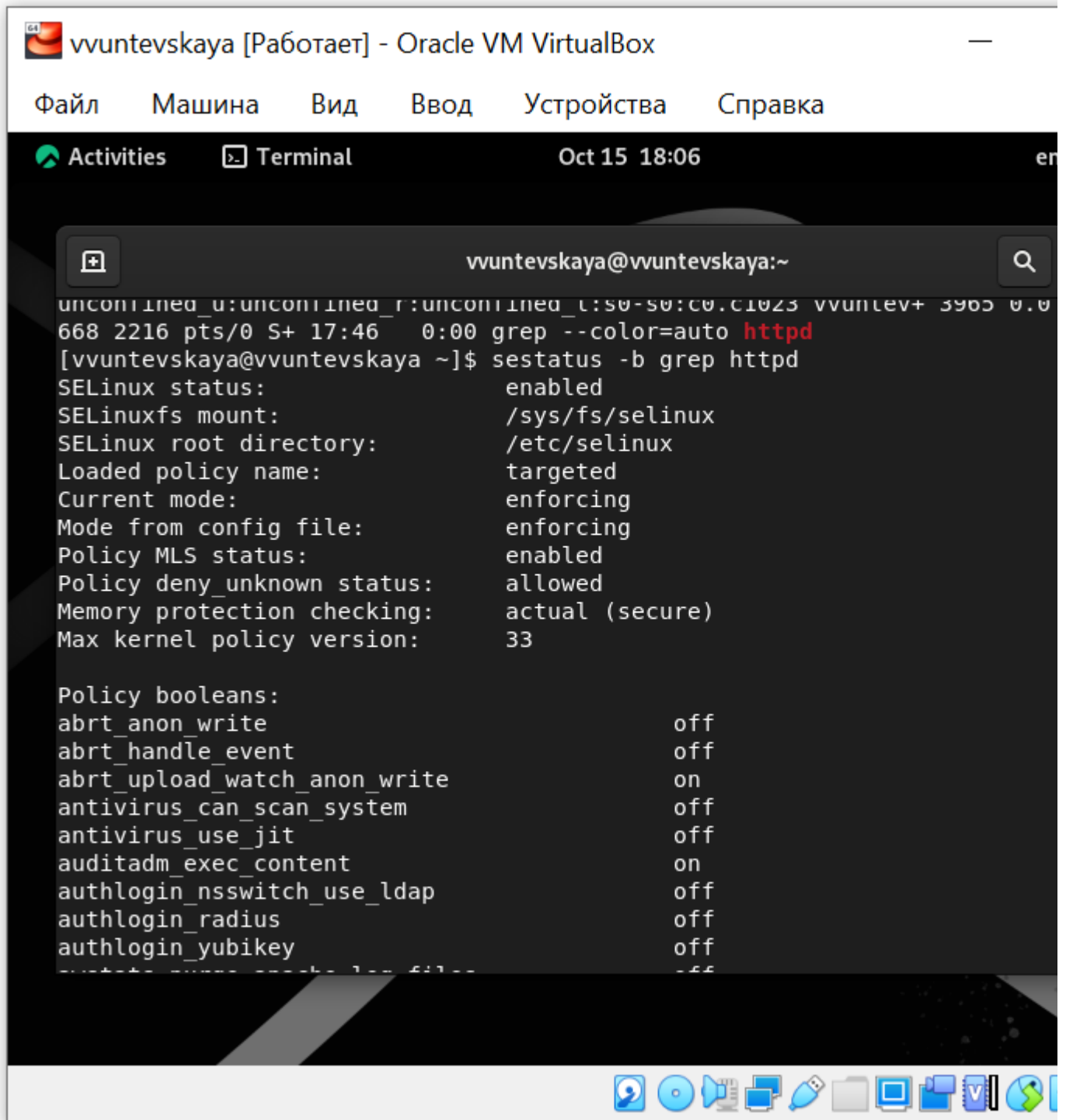
The screenshot shows a terminal window titled "vvuntevskaya [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

```
[vvuntevskaya@vvuntevskaya ~]$ getenforce
Enforcing
[vvuntevskaya@vvuntevskaya ~]$ 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
[vvuntevskaya@vvuntevskaya ~]$ 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; ver
   Active: active (running) since Sat 2022-10-15 17:35:00 MSK; 10min a
   Docs: man:httpd.service(8)
  Main PID: 3449 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0
   Tasks: 213 (limit: 12212)
  Memory: 23.1M
    CPU: 360ms
```

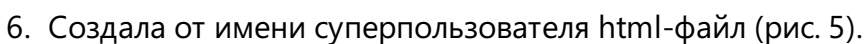
2. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности (рис. 2).

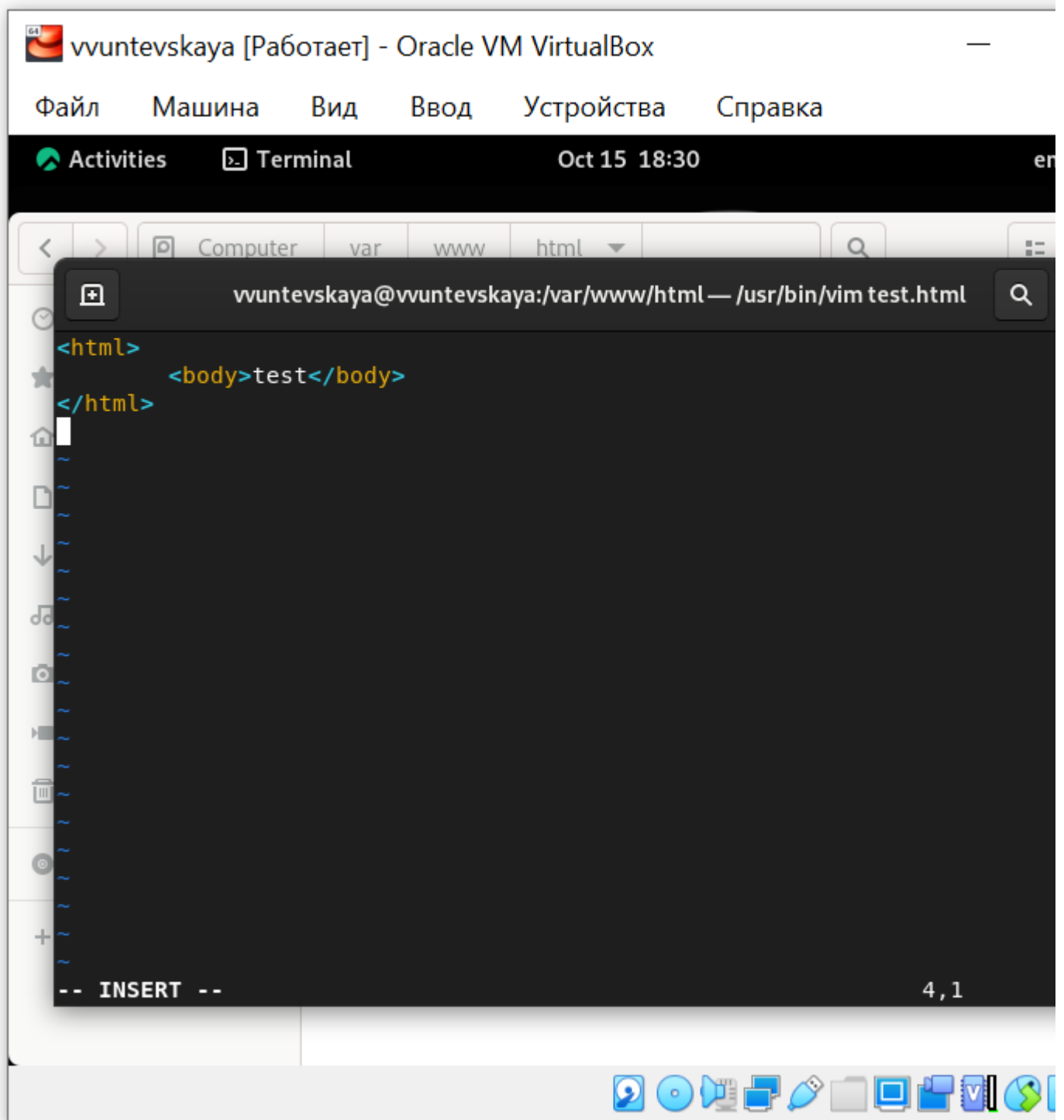


3. Посмотрела текущее состояние переключателей SELinux для Apache (рис. 3).

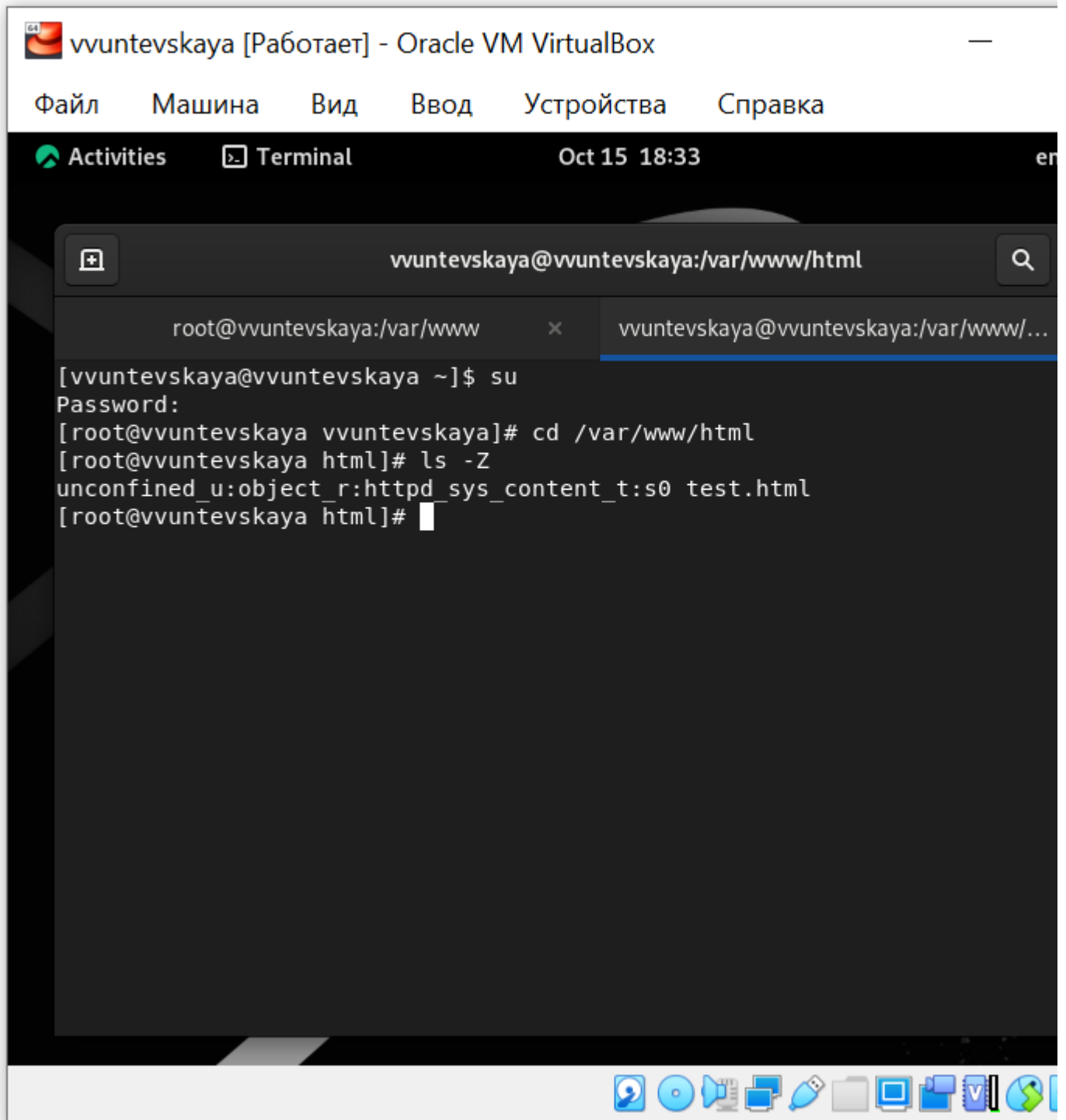


4. Посмотрела статистику по политике с помощью команды `seinfo`, также определила множество пользователей, ролей, типов.
5. Определила тип файлов и поддиректорий, находящихся в директории `/var/www`. Определила тип файлов, находящихся в директории `/var/www/html`. Определила круг пользователей, которым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

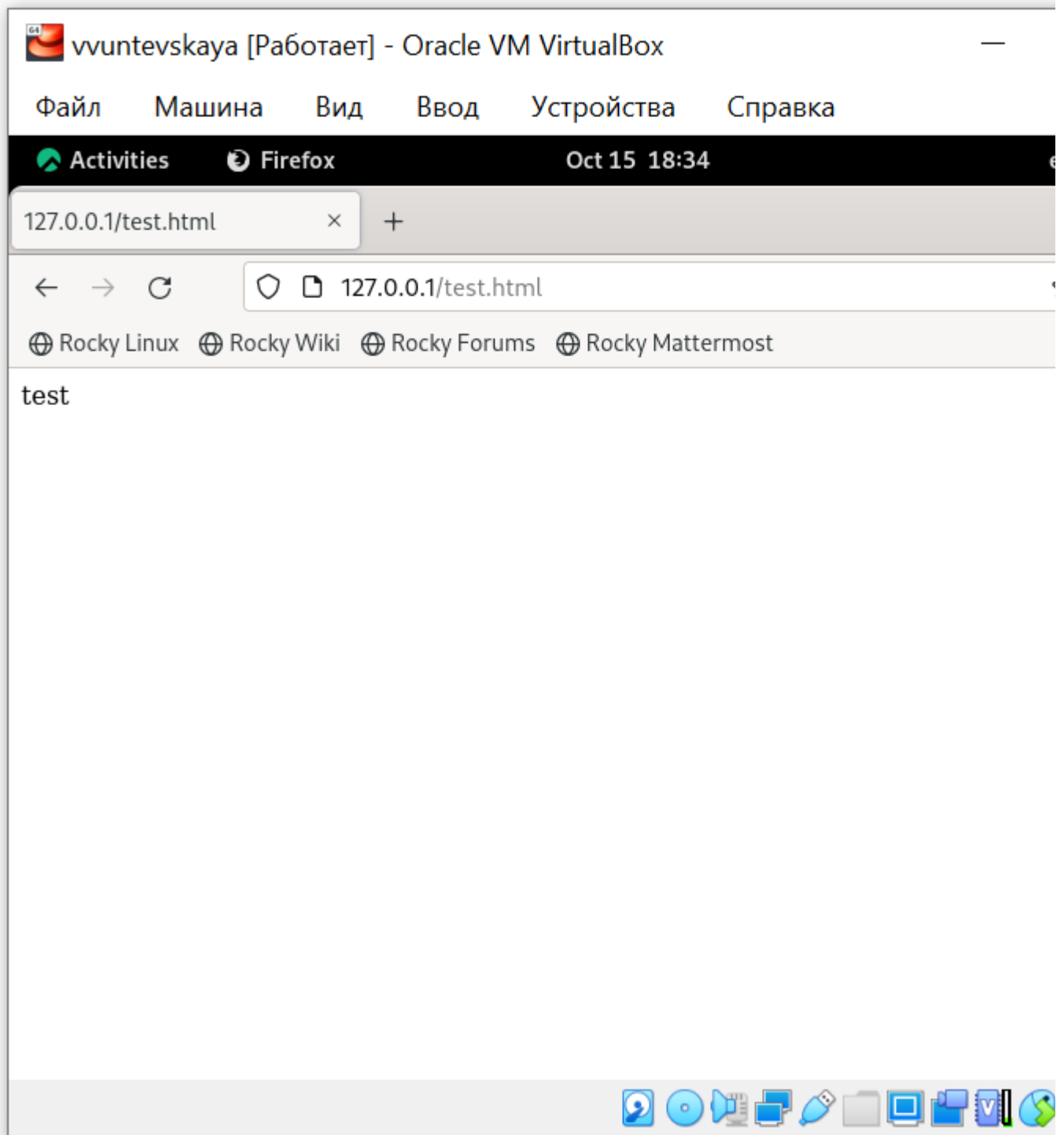




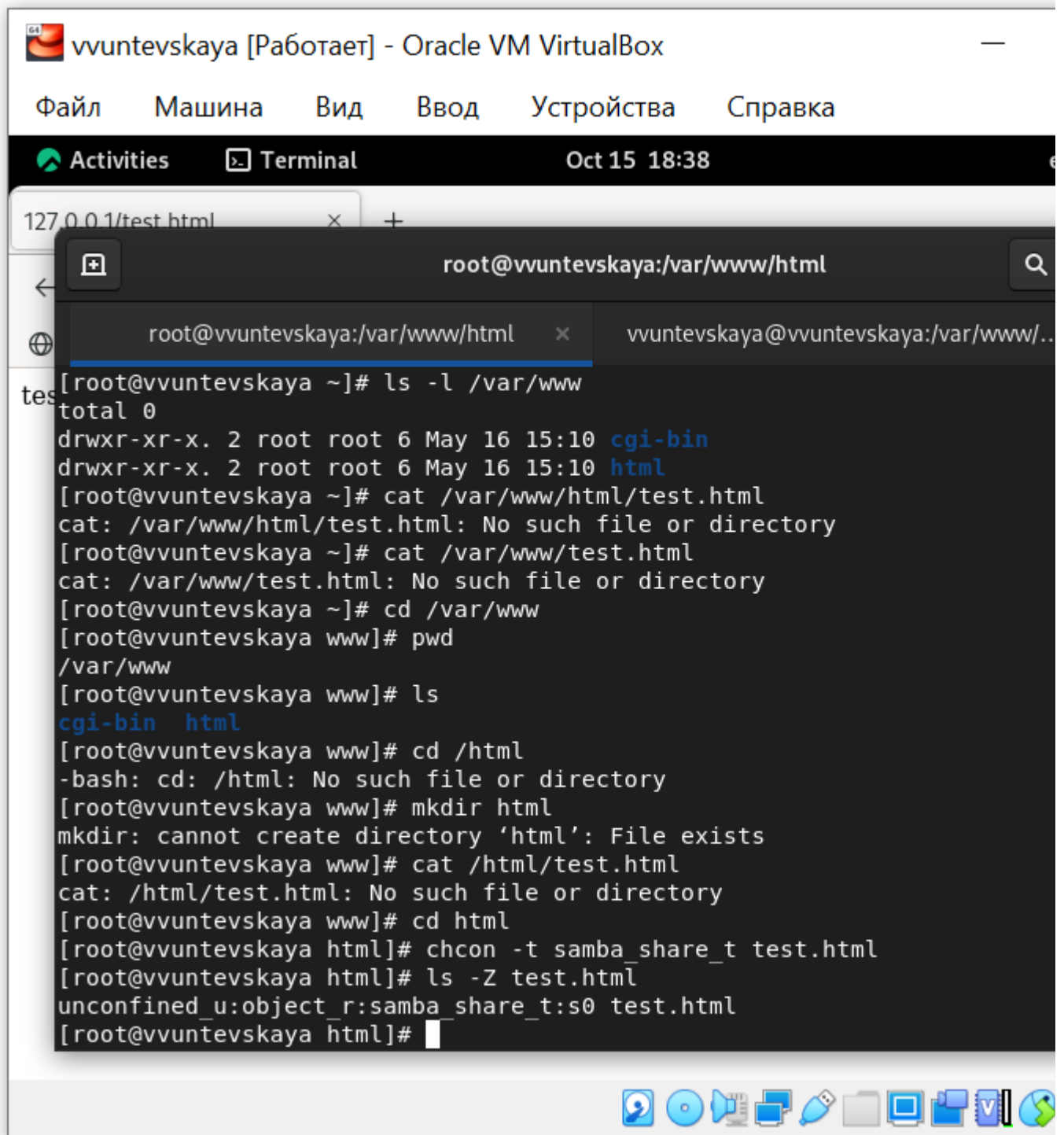
7. Проверила контекст созданного файла. Контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html: httpd_sys_content (рис. 6).



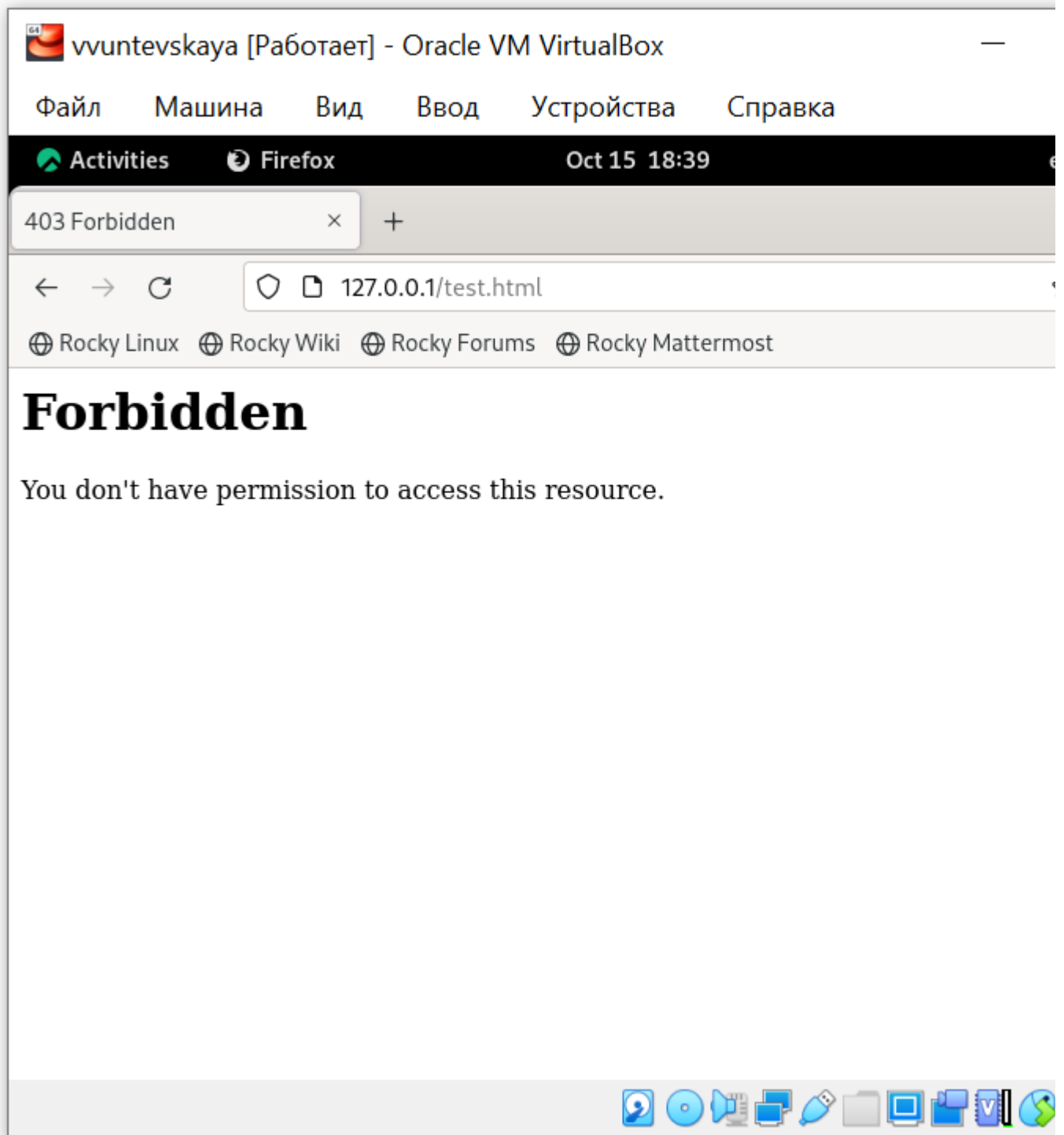
8. Обратилась к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедилась, что файл успешно отображён (рис. 7).



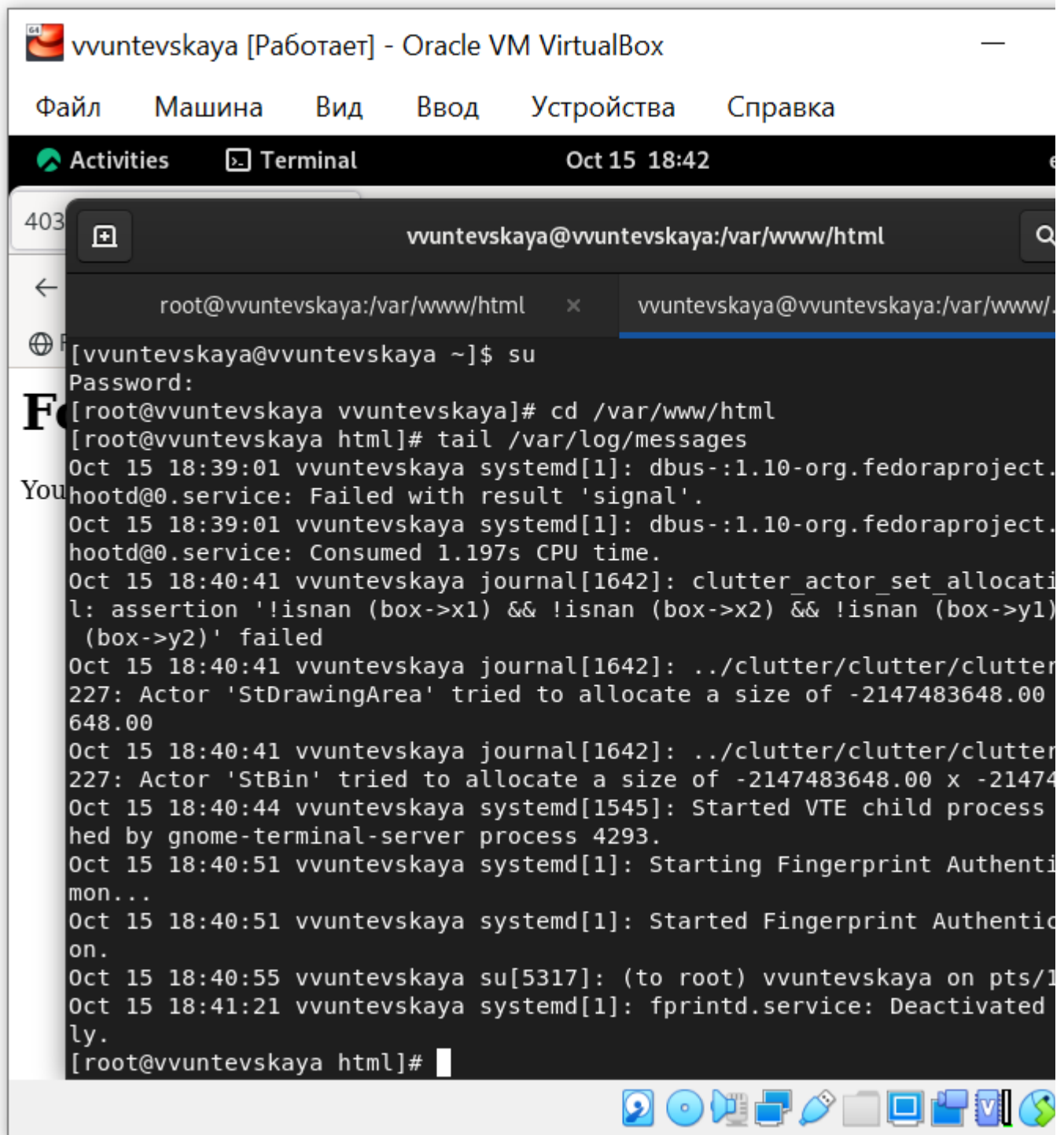
9. Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`. После этого проверила, что контекст поменялся (рис. 8).



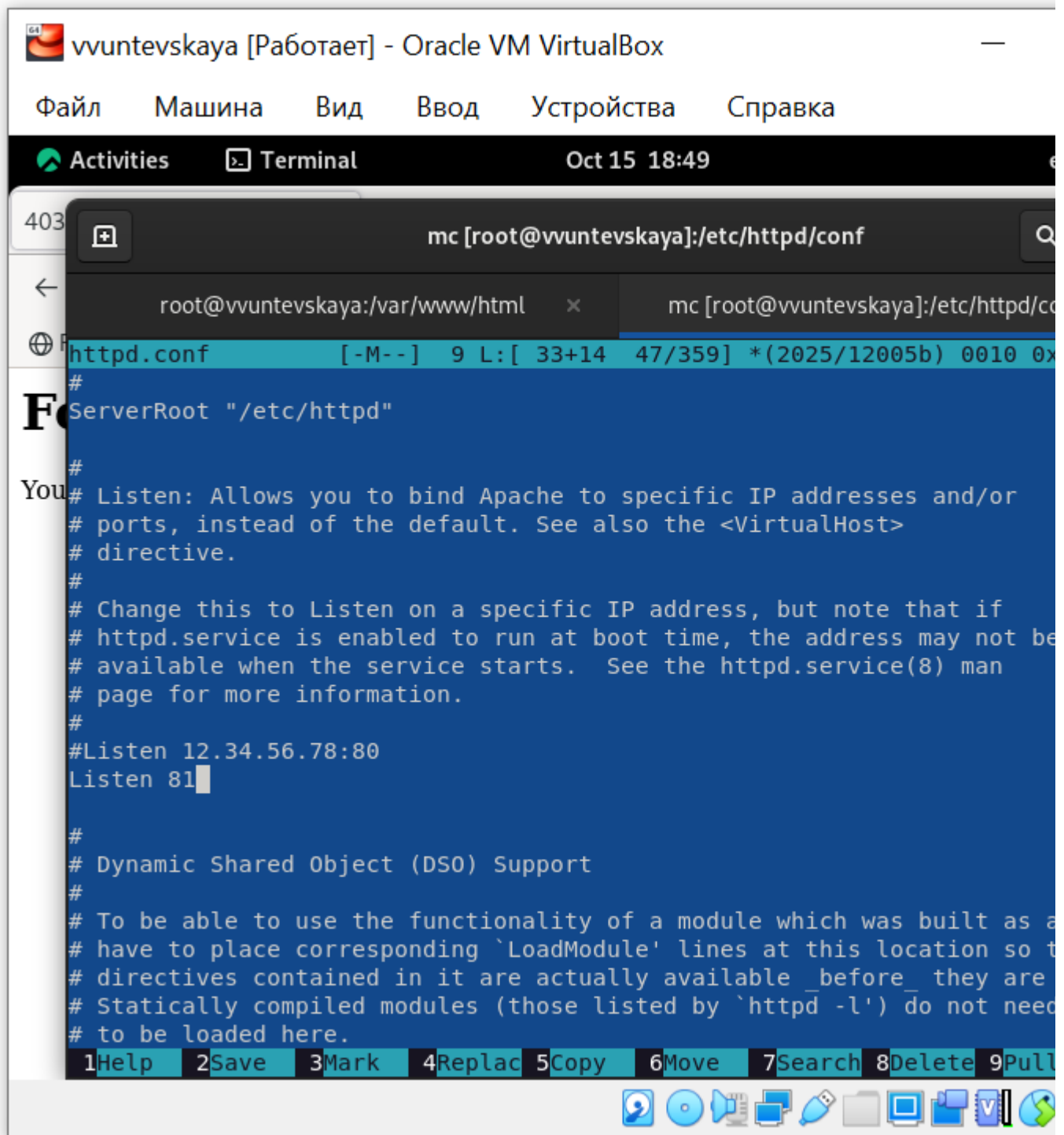
10. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html> (рис. 9).



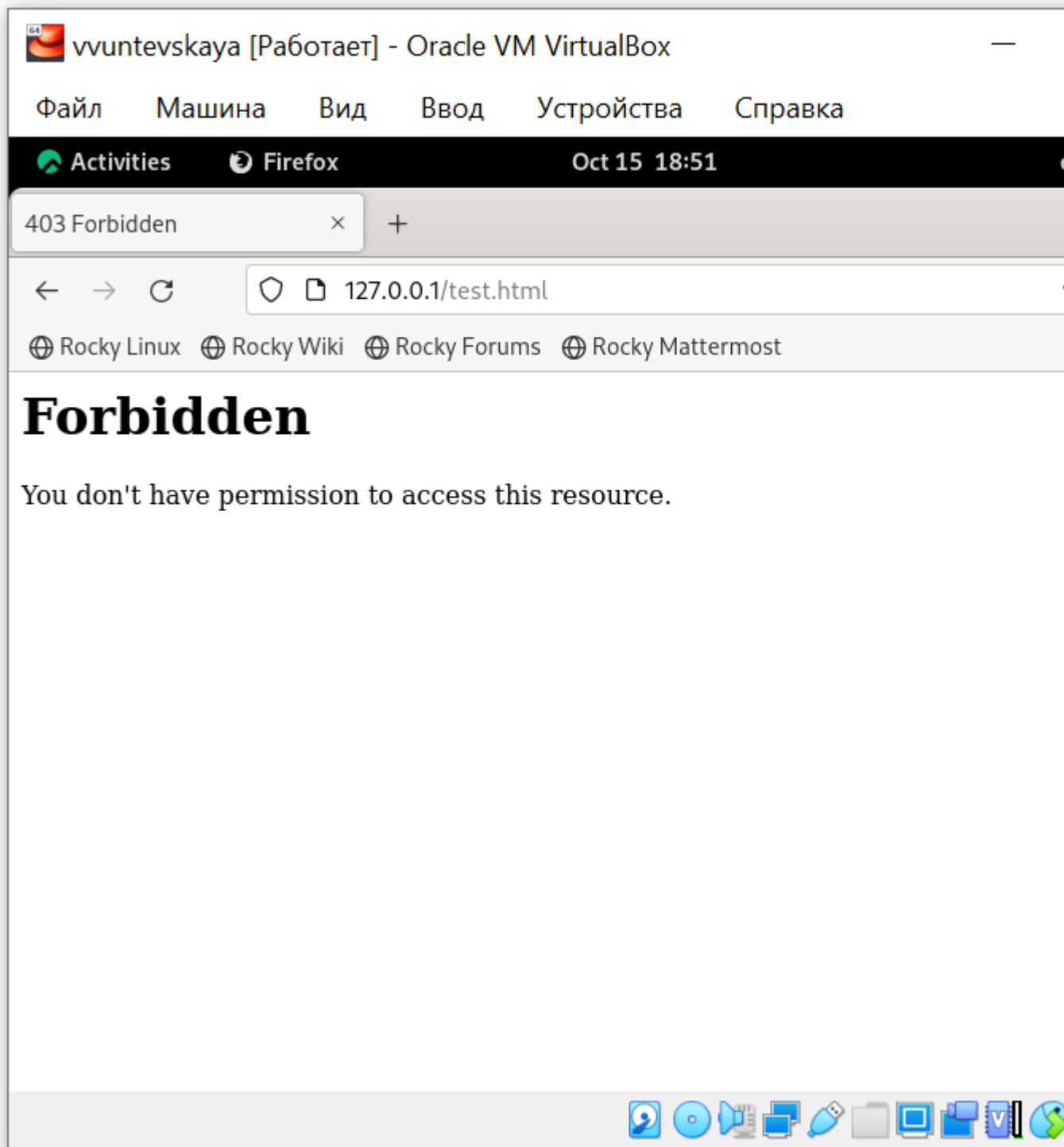
11. Проанализировала ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? Просмотрела log-файлы веб-сервера Apache. Также просмотрите системный лог-файл. Если в системе окажутся запущенными процессы `setroubleshootd` и `audtd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно (рис. 10).



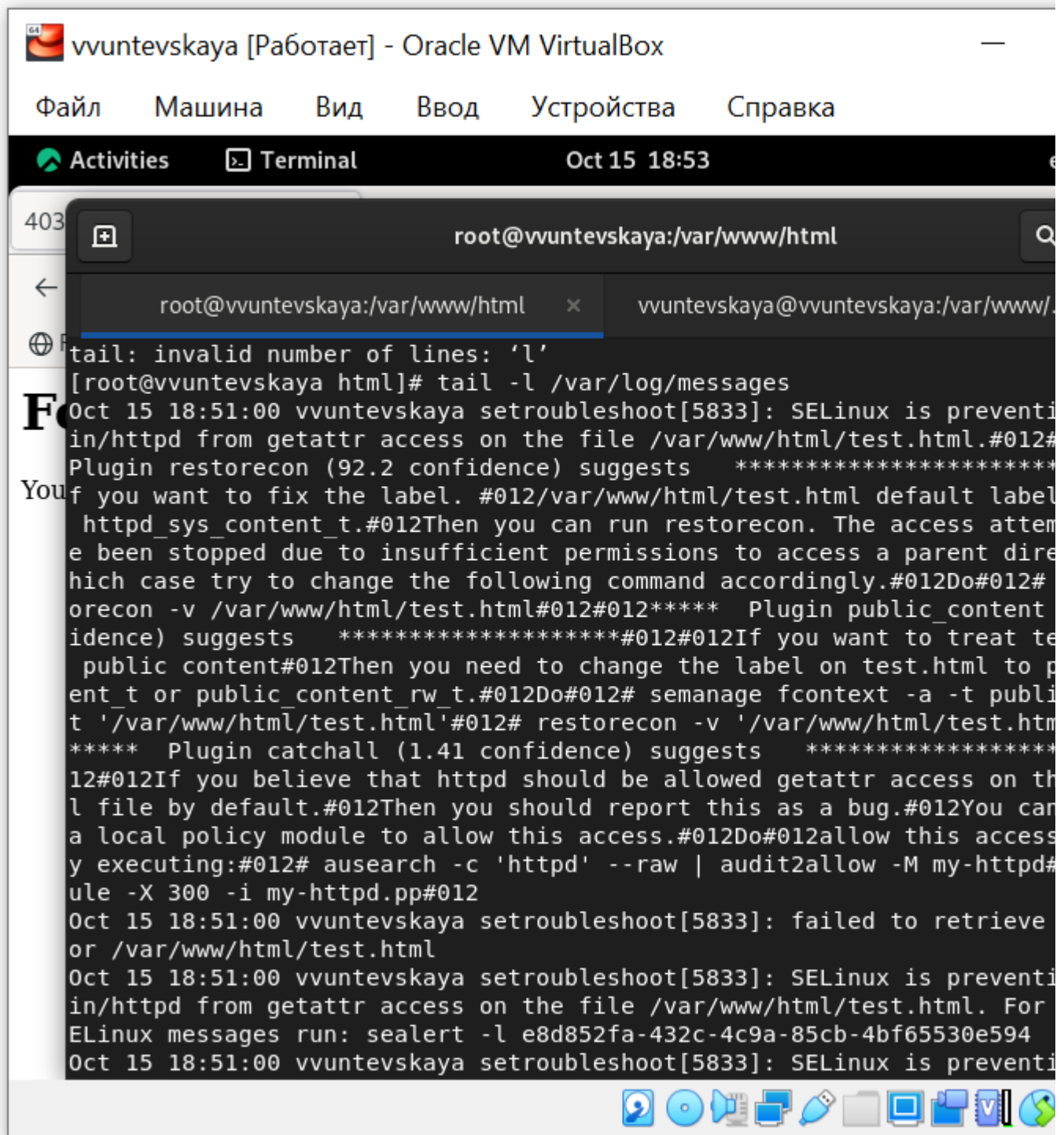
12. Попробовала запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле `/etc/httpd/httpd.conf` нашёл строчку `Listen 80` и заменил её на `Listen 81` (рис. 11).



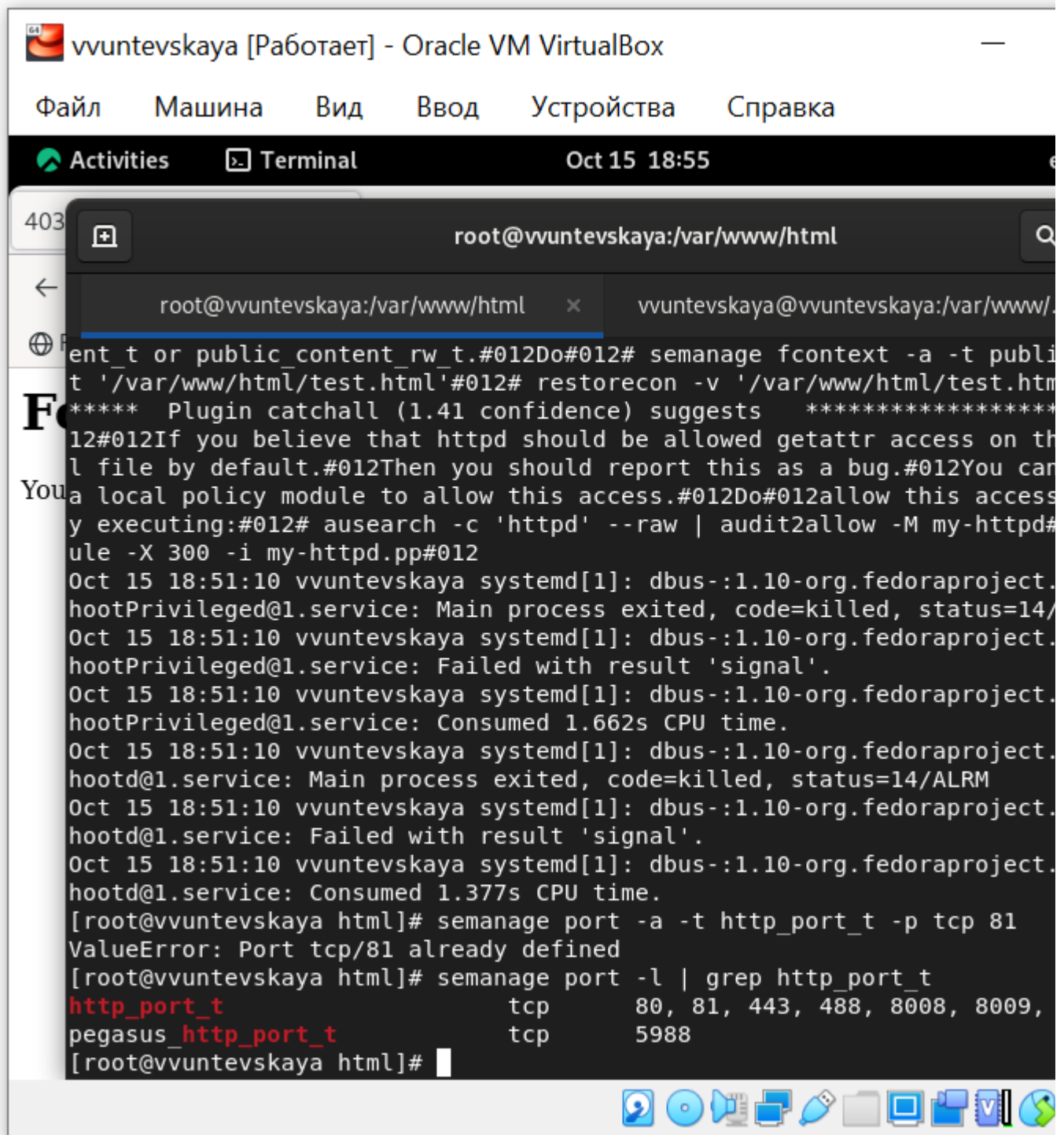
13. Выполнила перезапуск веб-сервера Apache. (рис. 12).



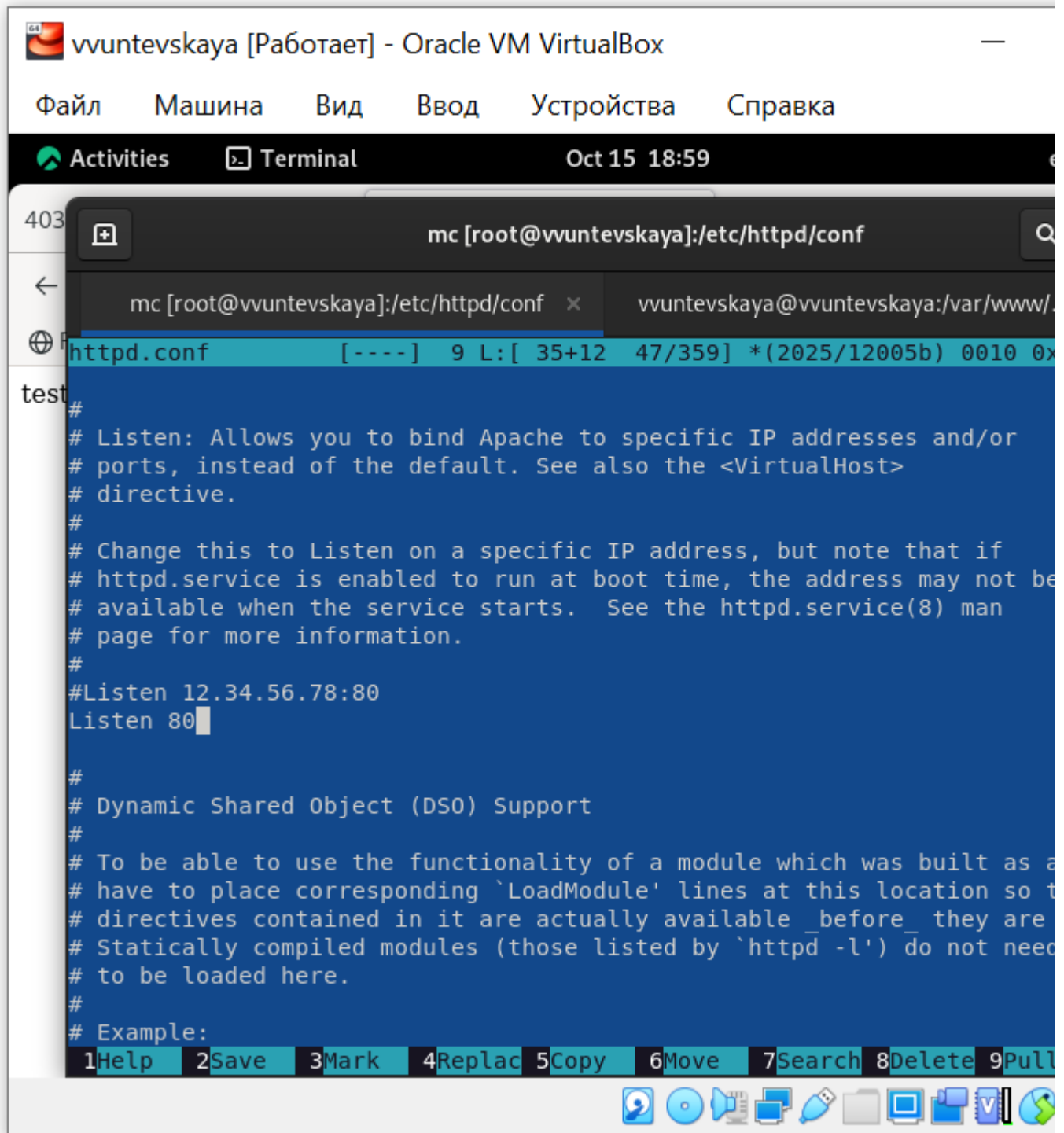
14. Проанализировала лог-файлы. Просмотрела файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` (рис. 13).



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).

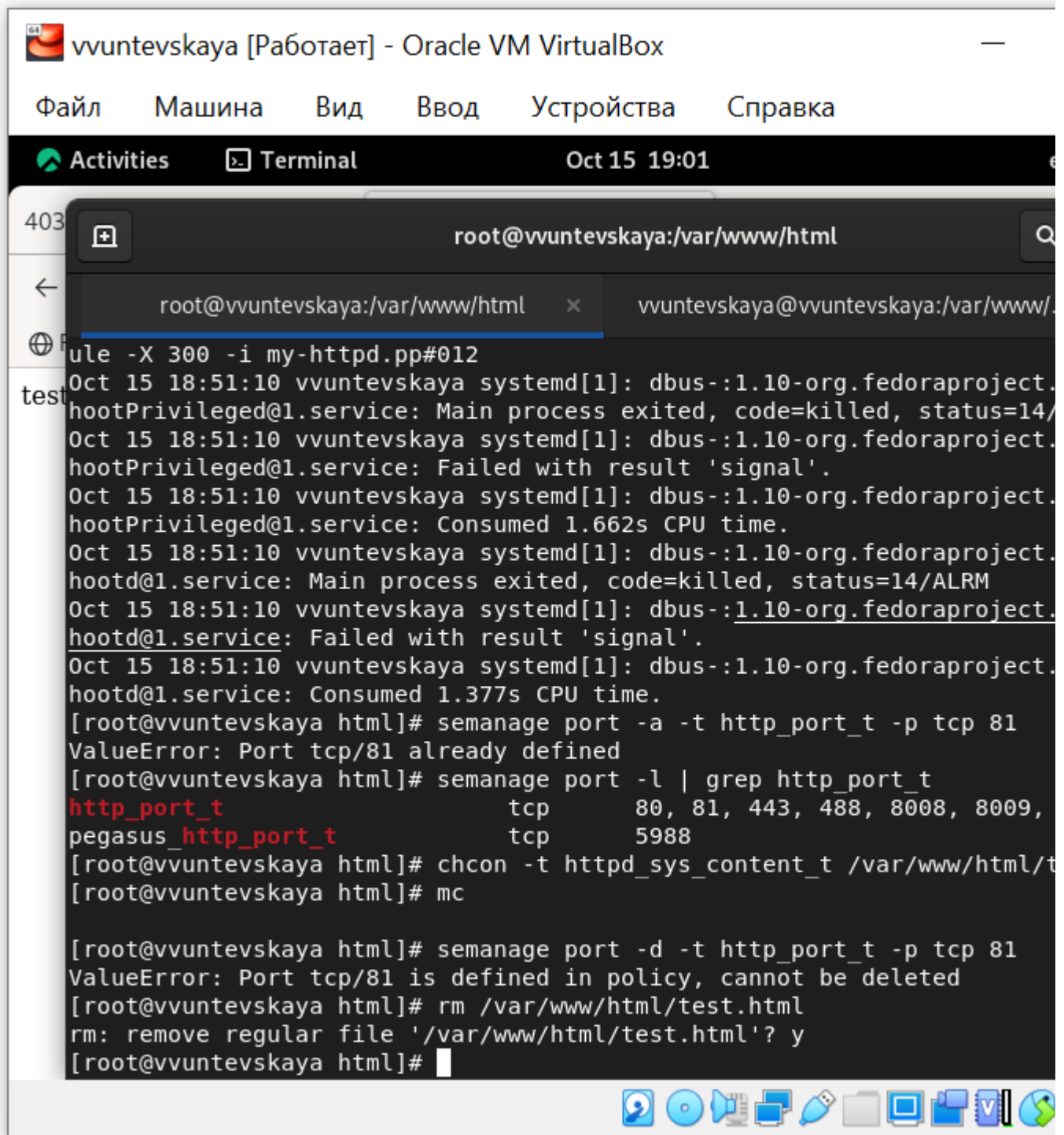


16. Вернула контекст httpd_sys_content_t к файлу /var/www/html/test.html (рис. 15).



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).



Выводы

Развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.

