

Отчёт по лабораторной работе 6

Радимов Игорь

Содержание

1 Цель работы	5
2 Задание	6
3 Подготовка	7
4 Выполнение лабораторной работы	9
5 Библиография	31
6 Выводы	32

List of Tables

List of Figures

3.1	рис.1. ServerName в httpd.conf.	7
3.2	рис.2. Отключение пакетного фильтра.	8
4.1	рис.3. Getenforce и sesstatus.	10
4.2	рис.4. Проверка работы веб-сервера.	10
4.3	рис.5. Список процессов.	11
4.4	рис.6. Переключатели SELinux для Apache.	11
4.5	рис.7. Seinfo.	12
4.6	рис.8. Определение типа файлов и круга пользователей.	13
4.7	рис.9. HTML код для веб сервера.	14
4.8	рис.10. Проверим контекст созданного файла.	15
4.9	рис.11. Браузер и веб-сервер.	16
4.10	рис.12. Лог файлы.	17
4.11	рис.13. Лог файлы(часть 2).	18
4.12	рис.14. Запрет доступа к веб-серверу.	19
4.13	рис.15. Анализ ситуации.	20
4.14	рис.16. Лог веб-сервера.	21
4.15	рис.17. Listen 81.	22
4.16	рис.18. Неудачная попытка соединения с веб-сервером через браузер.	23
4.17	рис.19. Перезапуск сервера.	24
4.18	рис.20. Лог.	25
4.19	рис.21. Лог(часть2).	26
4.20	рис.23. Список портов.	26
4.21	рис.24. Повторный перезапуск сервера.	27
4.22	рис.24. Удачная попытка доступа к серверу.	28
4.23	рис.25. Исправление конфигурационного файла.	29
4.24	рис.26. Удаление привязки и файла.	30

1 Цель работы

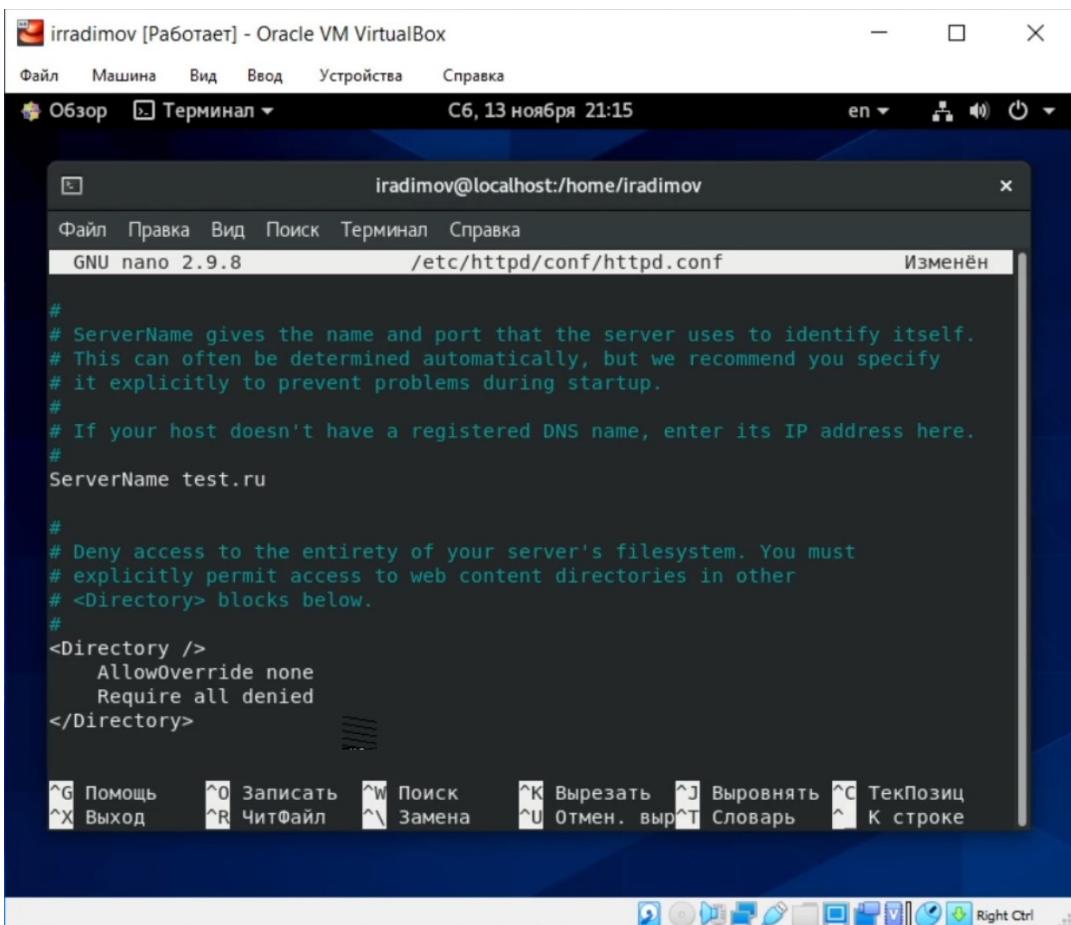
Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

2 Задание

Лабораторная работа подразумевает изучение влияния дополнительных атрибутов на файлы пользователя и изучение механизмов изменения идентификаторов.

3 Подготовка

1. В конфигурационном файле /etc/httpd/conf/httpd.conf задал параметр ServerName: ServerName test.ru



```
#  
# ServerName gives the name and port that the server uses to identify itself.  
# This can often be determined automatically, but we recommend you specify  
# it explicitly to prevent problems during startup.  
#  
# If your host doesn't have a registered DNS name, enter its IP address here.  
#  
ServerName test.ru  
  
#  
# Deny access to the entirety of your server's filesystem. You must  
# explicitly permit access to web content directories in other  
# <Directory> blocks below.  
#  
<Directory '/'>  
    AllowOverride none  
    Require all denied  
</Directory>
```

Figure 3.1: рис.1. ServerName в httpd.conf.

2. Проследил, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp.

Команды iptables -F и iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT

```
[root@localhost iradimov]# iptables -F
[root@localhost iradimov]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
Bad argument `iptables'
Try `iptables -h' or `iptables --help' for more information.
[root@localhost iradimov]# iptables -I tcp --dport 80 -j ACCEPT
iptables v1.8.4 (nf_tables): unknown option "--dport"
Try `iptables -h' or `iptables --help' for more information.
[root@localhost iradimov]#
```

Figure 3.2: рис.2. Отключение пакетного фильтра.

4 Выполнение лабораторной работы

1. Войдём в систему и убедимся что SELinux работает в режиме enforcing.

Убедимся что веб-сервер работает. Найдём веб-сервер Apache в списке процессов. Посмотрим текущее состояние переключателей SELinux для Apache.(рис 3-6)

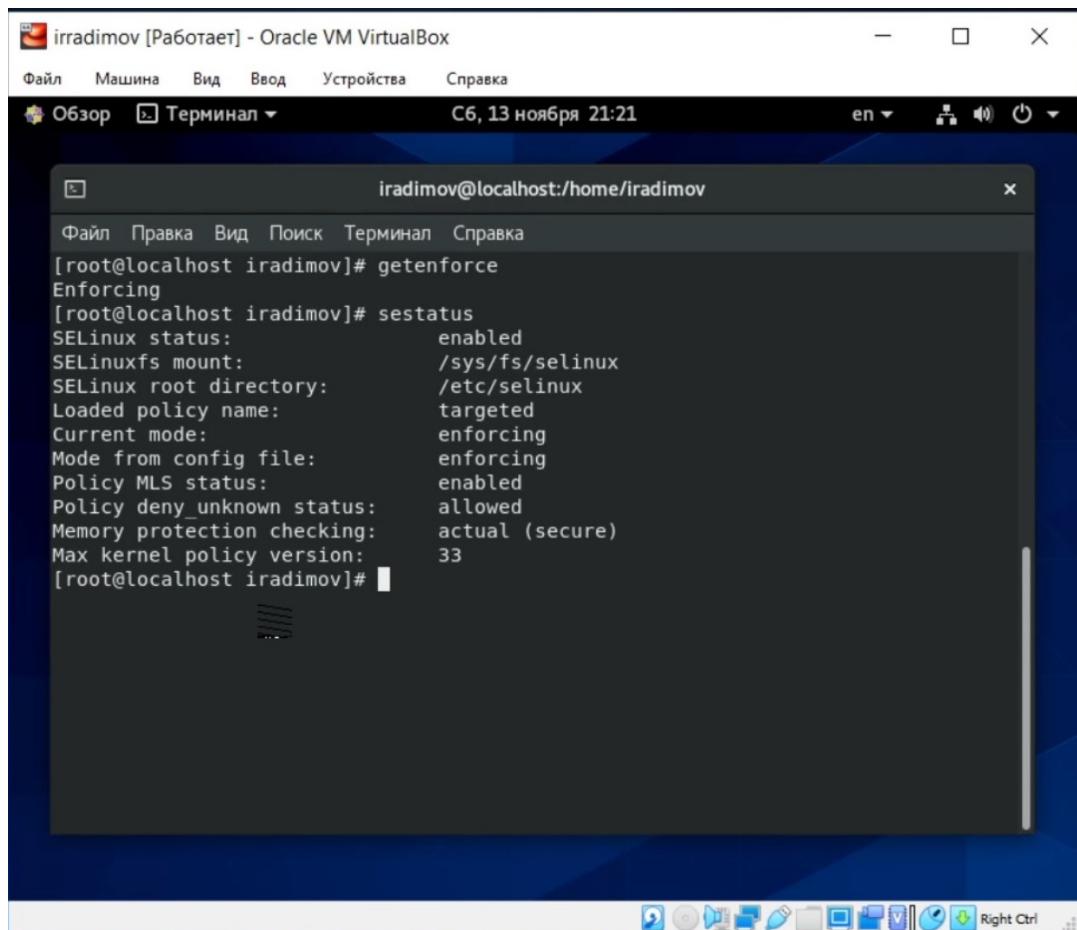


Figure 4.1: рис.3. Getenforce и sestatus.

```
[root@localhost iradimov]# 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 pres>
  Active: active (running) since Sat 2021-11-13 21:22:19 MSK; 6s ago
    Docs: man:httpd.service(8)
 Main PID: 3896 (httpd)
   Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 11252)
   Memory: 21.0M
  CGroup: /system.slice/httpd.service
          ├─3896 /usr/sbin/httpd -DFOREGROUND
          ├─3901 /usr/sbin/httpd -DFOREGROUND
          ├─3902 /usr/sbin/httpd -DFOREGROUND
          ├─3903 /usr/sbin/httpd -DFOREGROUND
          ├─3904 /usr/sbin/httpd -DFOREGROUND

ноя 13 21:22:19 localhost.localdomain systemd[1]: Starting The Apache HTTP Serv>
ноя 13 21:22:19 localhost.localdomain systemd[1]: Started The Apache HTTP Serve>
ноя 13 21:22:19 localhost.localdomain httpd[3896]: Server configured, listening>
lines 1-18/18 (END)
```

Figure 4.2: рис.4. Проверка работы веб-сервера.

```
[root@localhost iradimov]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root      3896  0.0  0.5 273832 11024 ?
Ss 21:22  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3901  0.0  0.4 289836  8228 ?
S 21:22  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3902  0.0  0.5 1347644 9864 ?
Sl 21:22  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3903  0.0  0.5 1347644 9872 ?
Sl 21:22  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    3904  0.0  0.5 1478772 9872 ?
Sl 21:22  0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 4152 0.0  0.0 221928
1044 pts/0 R+ 21:23  0:00 grep --color=auto httpd
[root@localhost iradimov]#
```

Figure 4.3: рис.5. Список процессов.

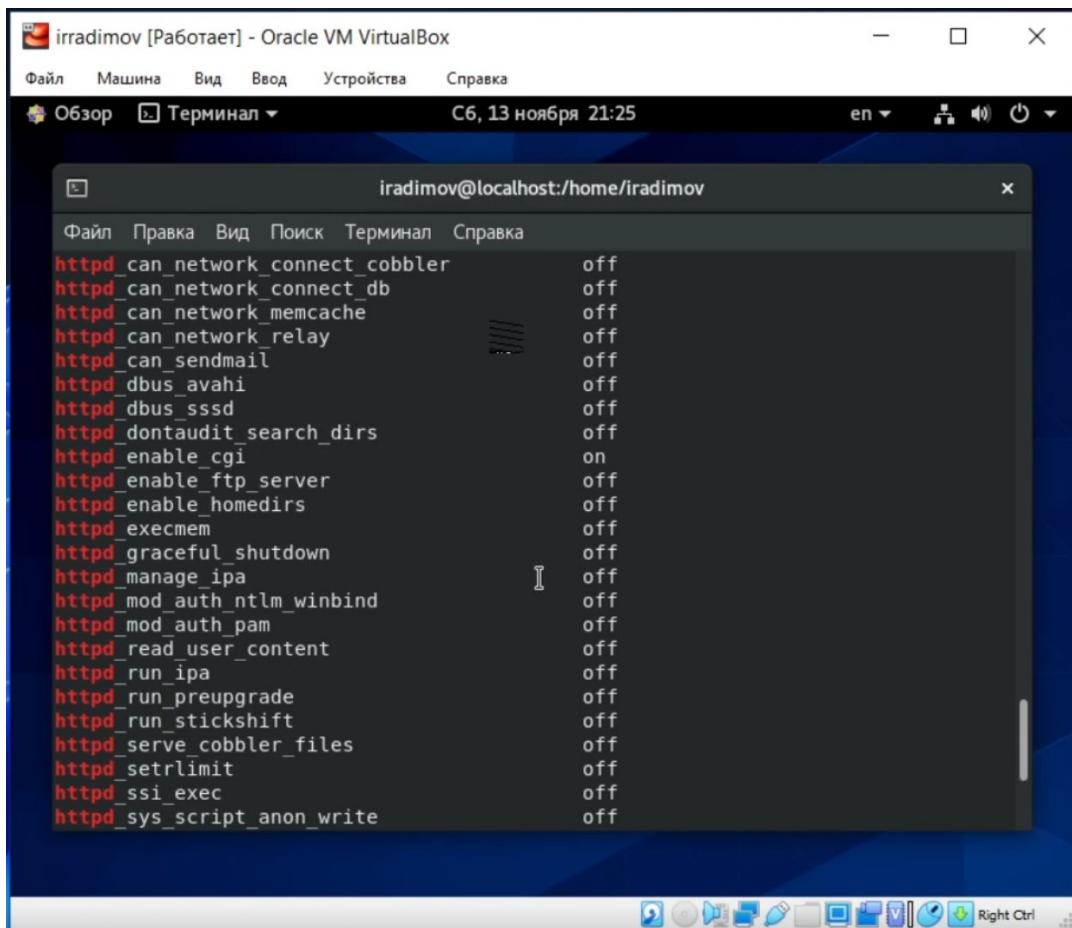
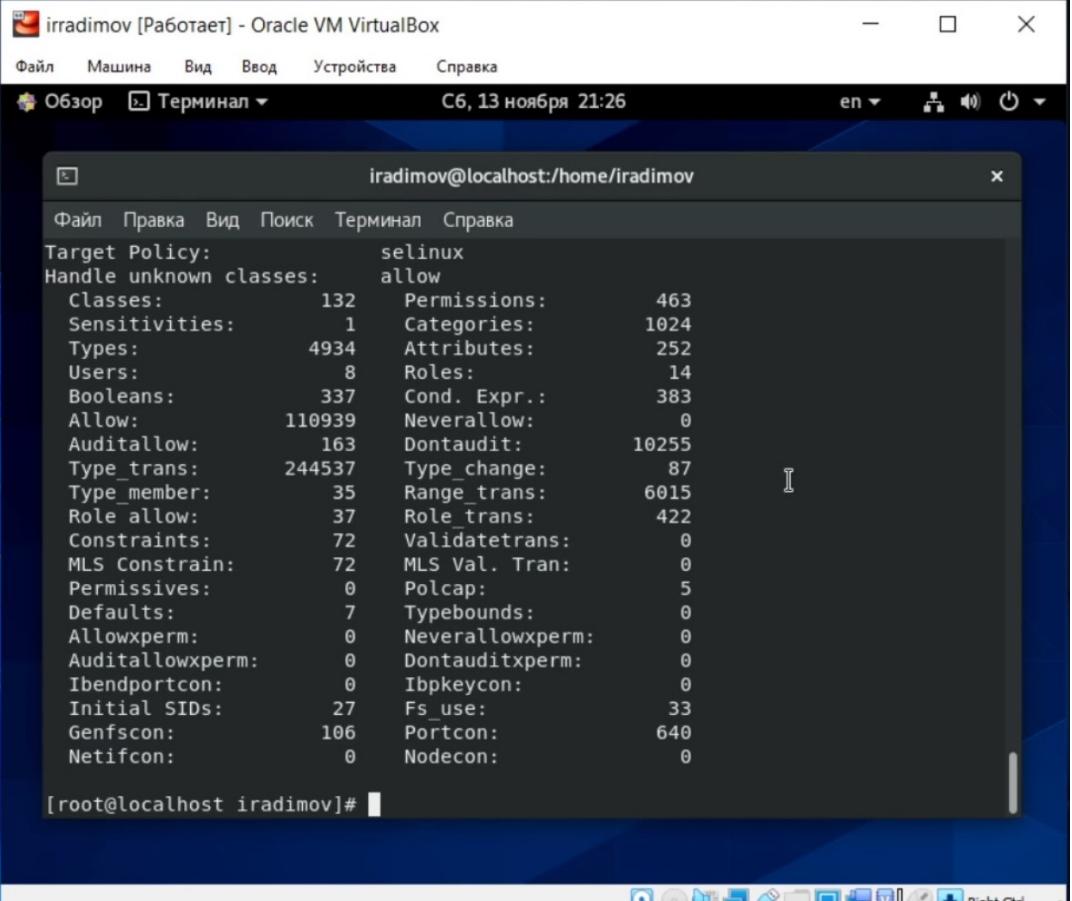


Figure 4.4: рис.6. Переключатели SELinux для Apache.

2. Посмотрим статистику по политике. Определим тип файлов и поддиректорий в /var/www и /var/www/html. Определим круг пользователей, которым разрешено создание файлов в директории /var/www/html.

Создадим от имени суперпользователя html файл. Проверим контекст созданного файла. (рис.7-10)

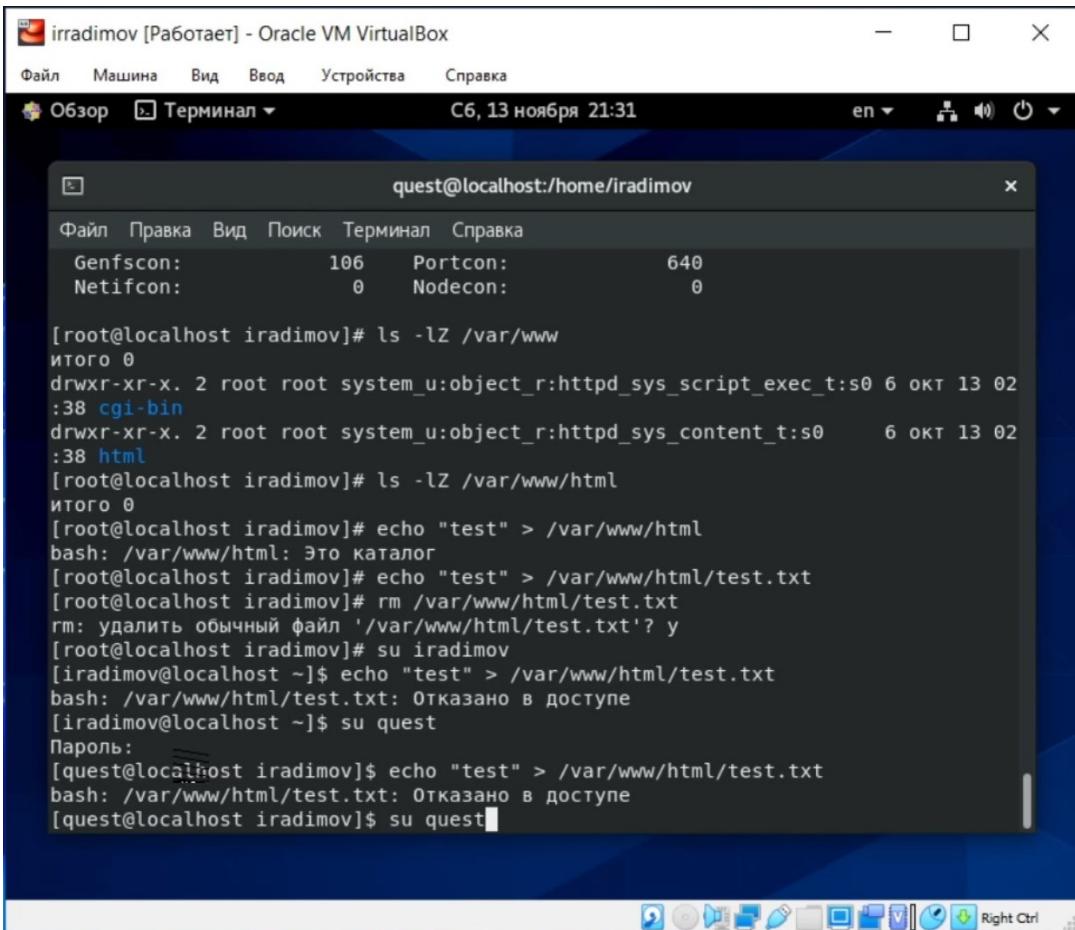


The screenshot shows a terminal window titled "iradimov@localhost:/home/iradimov" running on an Oracle VM VirtualBox machine. The window displays the output of the "seinfo" command, which provides detailed information about SELinux policy statistics. The output includes various counters for different policy components like classes, sensitivities, types, users, booleans, and various allow and audit flags. The terminal window has a dark theme and is part of a desktop environment with icons visible at the bottom.

```
Target Policy:           selinux
Handle unknown classes: allow
Classes:                132    Permissions:      463
Sensitivities:          1       Categories:        1024
Types:                  4934   Attributes:        252
Users:                  8       Roles:             14
Booleans:               337    Cond. Expr.:     383
Allow:                 110939  Neverallow:      0
Auditallow:              163   Dontaudit:       10255
Type_trans:              244537 Type_change:      87
Type_member:              35    Range_trans:     6015
Role allow:              37    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    Ibpkeycon:       0
Initial SIDs:             27   Fs_use:          33
Genfscon:                106  Portcon:        640
Netifcon:                0    Nodecon:         0

[root@localhost iradimov]#
```

Figure 4.5: рис.7. Seinfo.



Файл Машина Вид Ввод Устройства Справка

Обзор Терминал ▾ Сб, 13 ноября 21:31 en ▾

quest@localhost:/home/iradimov

```
Файл Правка Вид Поиск Терминал Справка
Genfscon: 106 Portcon: 640
Netifcon: 0 Nodecon: 0

[root@localhost iradimov]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 13 02
:38 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 окт 13 02
:38 html
[root@localhost iradimov]# ls -lZ /var/www/html
итого 0
[root@localhost iradimov]# echo "test" > /var/www/html
bash: /var/www/html: Это каталог
[root@localhost iradimov]# echo "test" > /var/www/html/test.txt
[root@localhost iradimov]# rm /var/www/html/test.txt
rm: удалить обычный файл '/var/www/html/test.txt'? y
[root@localhost iradimov]# su iradimov
[iradimov@localhost ~]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[iradimov@localhost ~]$ su quest
Пароль:
[quest@localhost iradimov]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[quest@localhost iradimov]$ su quest
```

Figure 4.6: рис.8. Определение типа файлов и круга пользователей.

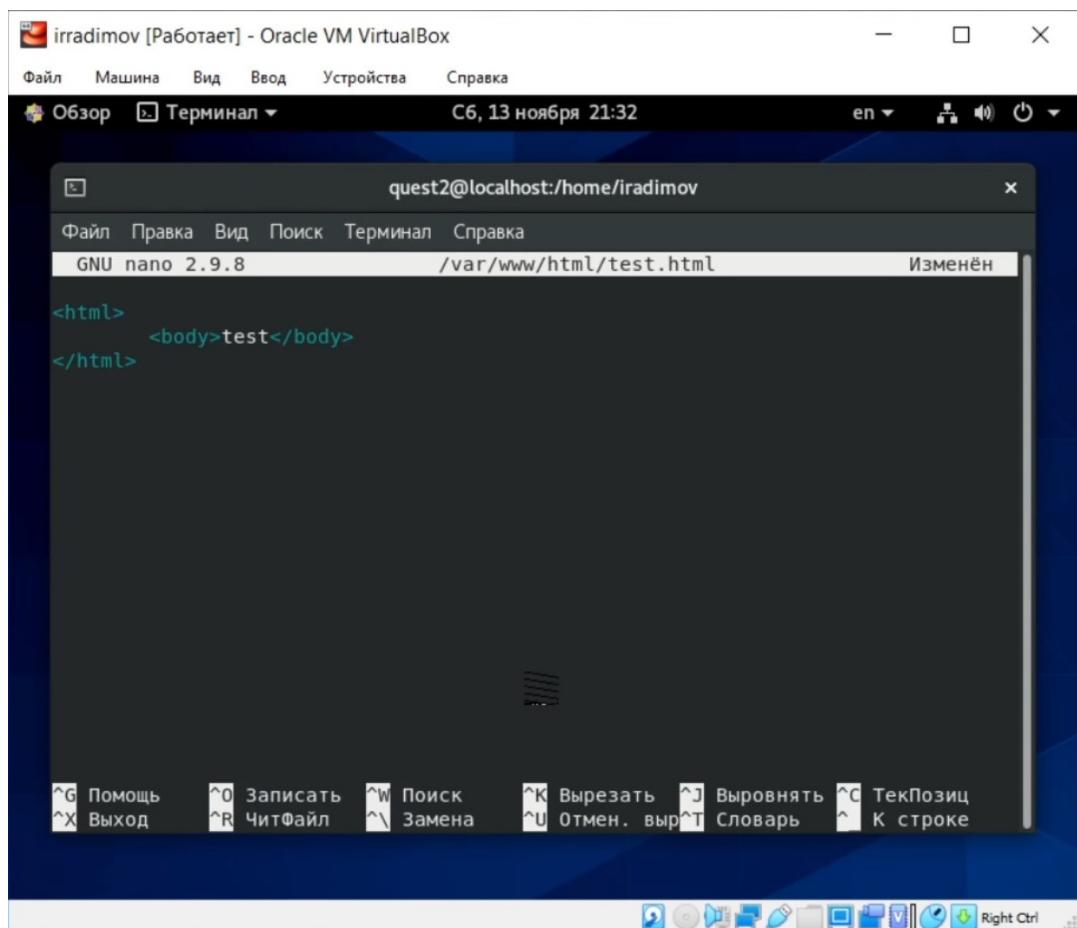


Figure 4.7: рис.9. HTML код для веб сервера.

```
[root@localhost iradimov]# echo "test" > /var/www/html/test
bash: /var/www/html: Это каталог
[root@localhost iradimov]# echo "test" > /var/www/html/test.txt
[root@localhost iradimov]# rm /var/www/html/test.txt
rm: удалить '/var/www/html/test.txt'? y
[root@localhost iradimov]# su iradimov
[iradimov@localhost ~]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[iradimov@localhost ~]$ su quest
Пароль:
[quest@localhost iradimov]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[quest@localhost iradimov]$ su quest2
Пароль:
[quest2@localhost iradimov]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[quest2@localhost iradimov]$ su
Пароль:
[root@localhost iradimov]# nano /var/www/html/test.html
[root@localhost iradimov]# ls -lZ /var/www/html
итого 4
-rw-r--r-- 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 ноя 13 2
1:32 test.html
[root@localhost iradimov]#
```

Figure 4.8: рис.10. Проверим контекст созданного файла.

3. Обратимся к файлу через веб-сервер и убедимся, что файл был успешно отображен. Выясним какие контексты файлов определены для httpd. Изменим контекст файла test.html . Попробуем ещё раз получить доступ к файлу через веб-сервер, но получим сообщение об ошибке.(рис.11-15)

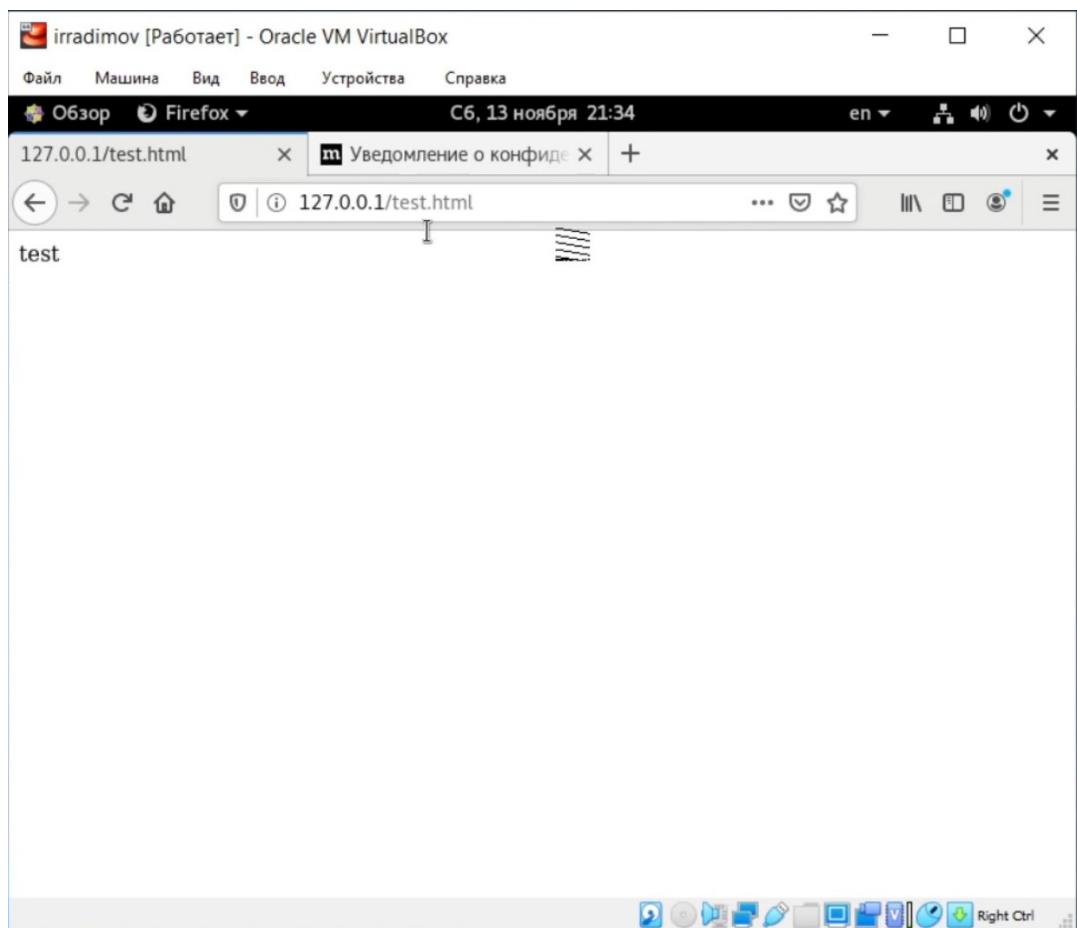


Figure 4.9: рис.11. Браузер и веб-сервер.

The screenshot shows a terminal window titled "quest2@localhost:/home/iradimov" running within an Oracle VM VirtualBox environment. The terminal session logs the following commands and their results:

```
echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
su quest
Пароль:
echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
su quest2
Пароль:
echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
su
Пароль:
nano /var/www/html/test.html
ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 ноя 13 2
1:32 test.html
ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 ноя 13 2
1:32 /var/www/html/test.html
chcon -t samba_share_t /var/www/html/test.html
ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Figure 4.10: рис.12. Лог файлы.

The screenshot shows a terminal window titled 'Terminál' (Terminal) in Russian, running on a host system with the IP address 127.0.0.1/test.html. The terminal session is connected to a guest machine at localhost with the user 'quest2'. The log output shows several attempts to write to the file '/var/www/html/test.txt' from different users (iradimov, quest, quest2) and as root, all of which fail with the message 'Отказано в доступе' (Access denied). It also shows the creation of a file 'test.html' and its chmod and chcon commands to set it as a Samba share.

```
Файл Правка Вид Поиск Терминал Справка
[iradimov@localhost ~]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[iradimov@localhost ~]$ su quest
Пароль:
[quest@localhost iradimov]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[quest@localhost iradimov]$ su quest2
Пароль:
[quest2@localhost iradimov]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[quest2@localhost iradimov]$ su
Пароль:
[root@localhost iradimov]# nano /var/www/html/test.html
[root@localhost iradimov]# ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 ноя 13 2
1:32 test.html
[root@localhost iradimov]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 ноя 13 2
1:32 /var/www/html/test.html
[root@localhost iradimov]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost iradimov]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@localhost iradimov]#
```

Figure 4.11: рис.13. Лог файлы(часть 2).

The screenshot shows a terminal window titled "403 Forbidden" running on a Linux system. The terminal session is as follows:

```
[iradimov@localhost ~]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[iradimov@localhost ~]$ su quest
Пароль:
[quest@localhost iradimov]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[quest@localhost iradimov]$ su
Пароль:
[root@localhost iradimov]# nano /var/www/html/test.html
[root@localhost iradimov]# ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 ноя 13 2
1:32 test.html
[root@localhost iradimov]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 ноя 13 2
1:32 /var/www/html/test.html
[root@localhost iradimov]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost iradimov]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@localhost iradimov]# tail /var/log/me
```

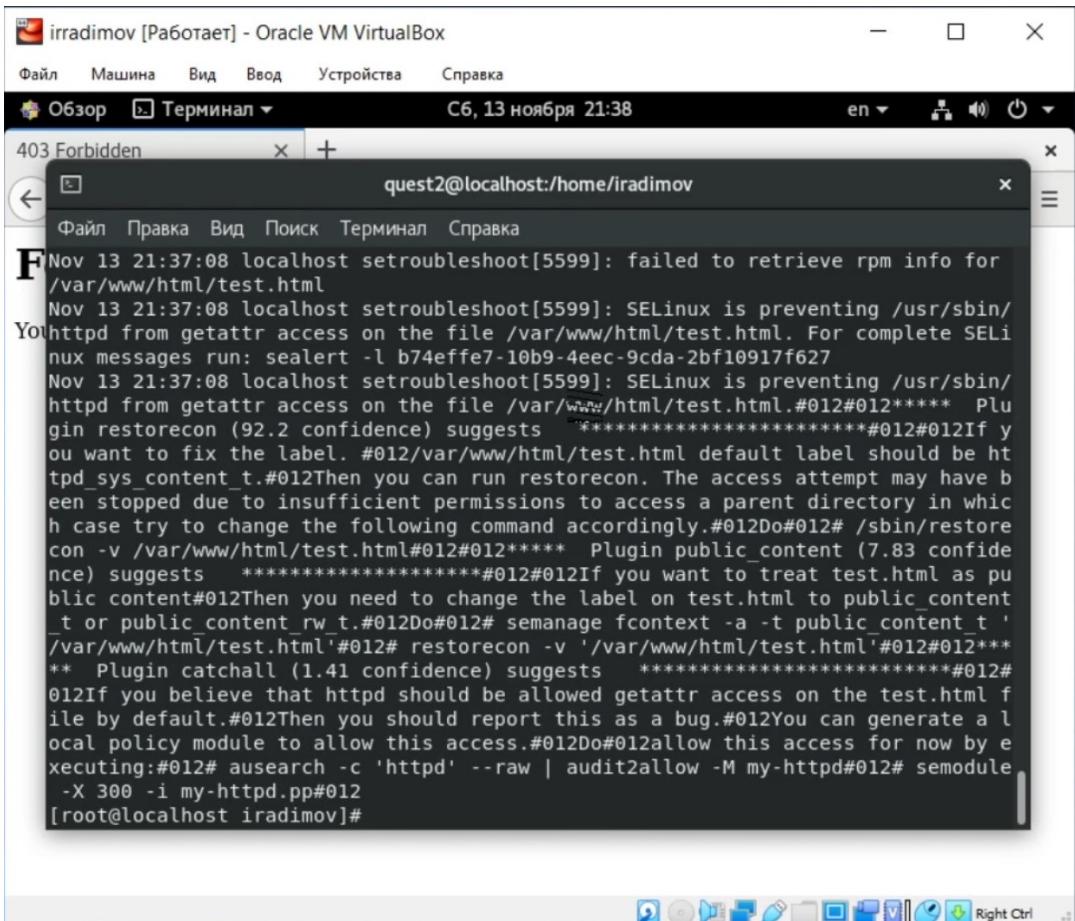
Figure 4.12: рис.14. Запрет доступа к веб-серверу.

The screenshot shows a terminal window titled '403 Forbidden' with the URL 'quest2@localhost:/home/iradimov'. The terminal window is part of a desktop environment with a menu bar at the top. The terminal content shows a user named 'iradimov' attempting to write to a file ('test.txt') in the '/var/www/html' directory, which is denied due to permission issues. The user then switches to another user ('quest') and attempts the same operation, also denied. Finally, the user becomes root ('root') and performs several administrative tasks: creating a new file ('test.html'), listing files with extended attributes ('ls -lZ'), changing file contexts ('chcon'), and listing files again ('ls -Z').

```
F [iradimov@localhost ~]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[iradimov@localhost ~]$ su quest
You need root privileges to run this command.
Пароль:
[quest@localhost iradimov]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[quest2@localhost iradimov]$ su
Пароль:
[root@localhost iradimov]# nano /var/www/html/test.html
[root@localhost iradimov]# ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 ноя 13 2
1:32 test.html
[root@localhost iradimov]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 ноя 13 2
1:32 /var/www/html/test.html
[root@localhost iradimov]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost iradimov]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@localhost iradimov]# ta
```

Figure 4.13: рис.15. Анализ ситуации.

4. Посмотрим лог файлы веб-сервера Apache. Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81. Выполним перезапуск(получен сбой). (рис.16-19)



The screenshot shows a terminal window titled 'quest2@localhost:/home/iradimov' running within an Oracle VM VirtualBox environment. The window displays a log of SELinux audit messages from the 'setroubleshoot' service. The log entries are as follows:

```
Nov 13 21:37:08 localhost setroubleshoot[5599]: failed to retrieve rpm info for /var/www/html/test.html
Nov 13 21:37:08 localhost setroubleshoot[5599]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l b74effe7-10b9-4eec-9cda-2bf10917f627
Nov 13 21:37:08 localhost setroubleshoot[5599]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent directory in which case try to change the following command accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012*** Plugin catchall (1.41 confidence) suggests *****#012#012If you believe that httpd should be allowed getattr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by executing:#012#ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
[root@localhost iradimov]#
```

Figure 4.14: рис.16. Лог веб-сервера.

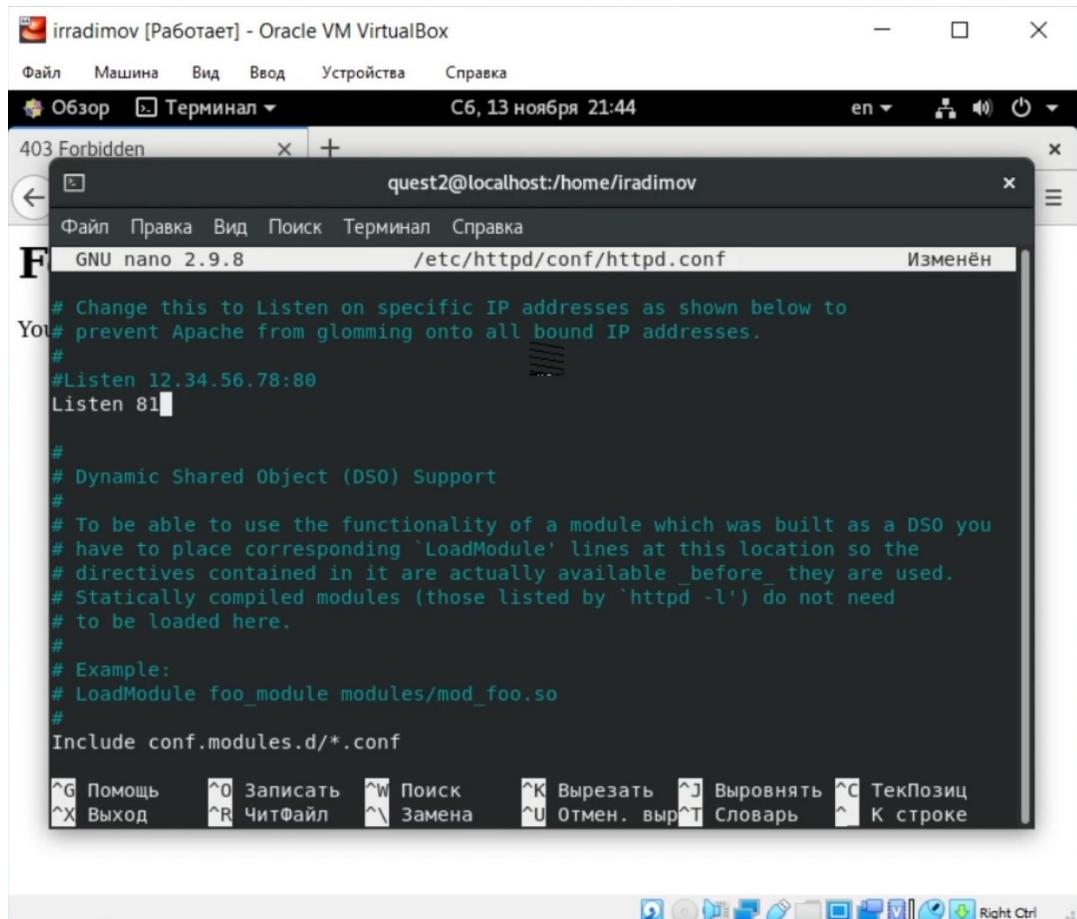


Figure 4.15: рис.17. Listen 81.

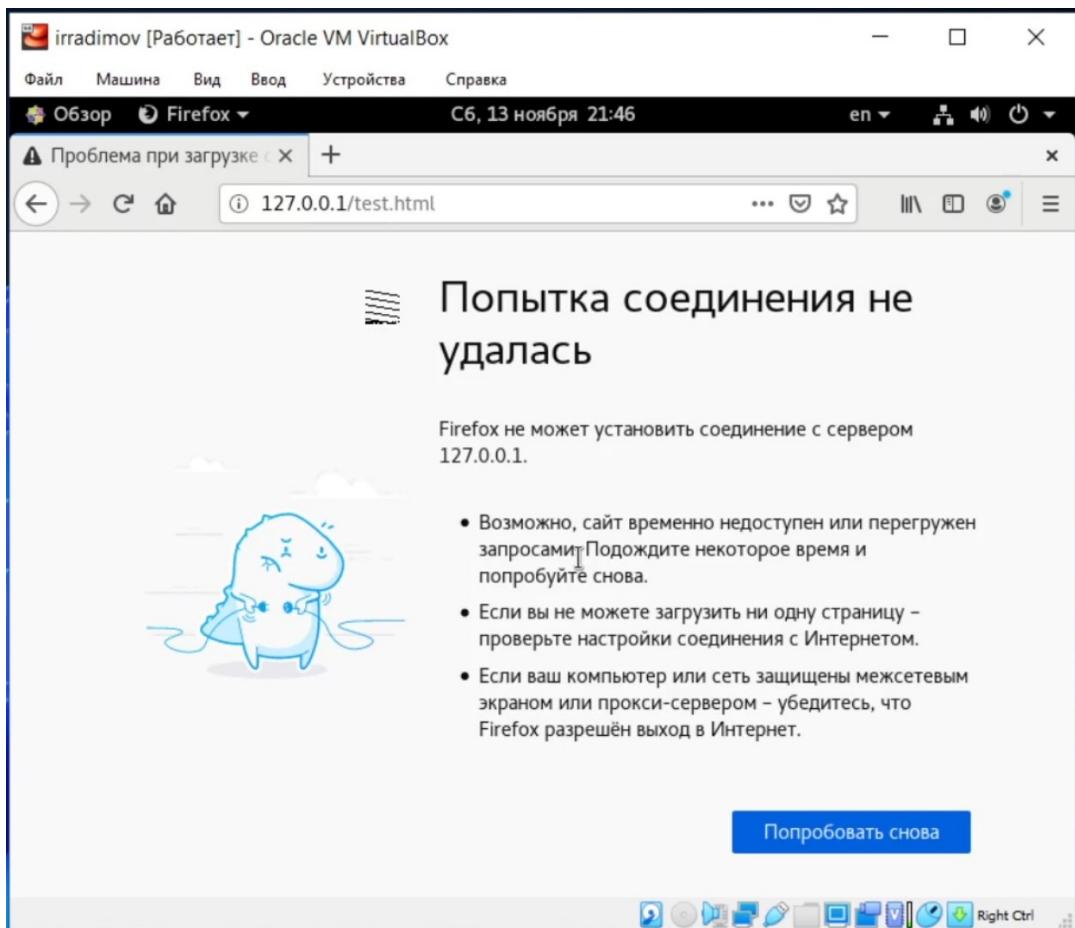
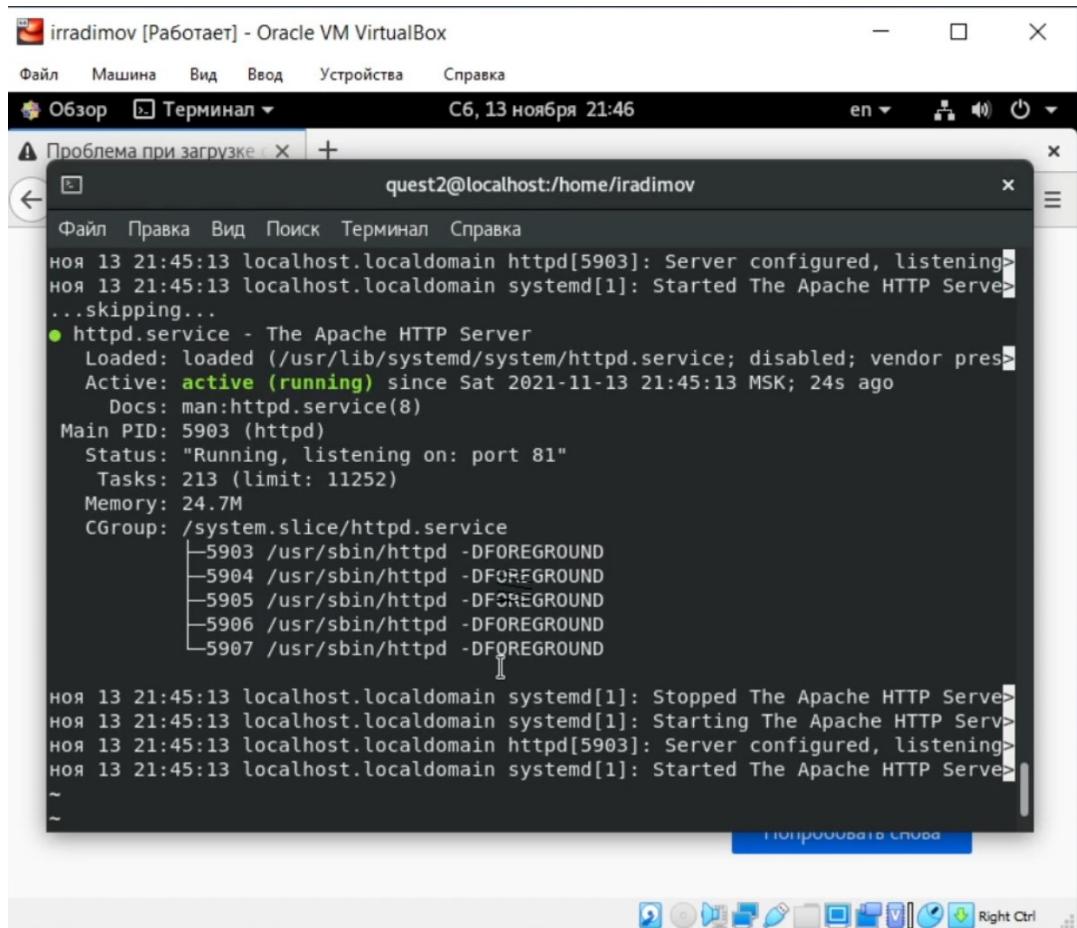


Figure 4.16: рис.18. Неудачная попытка соединения с веб-сервером через браузер.



The screenshot shows a terminal window titled 'quest2@localhost:/home/iradimov' running on an Oracle VM VirtualBox machine named 'irradimov [Работает]'. The terminal displays log messages from the Apache HTTP Server. The log entries show the server being configured, listening on port 81, and then being stopped and started again. The Apache service is listed as active (running) with a main PID of 5903.

```
ноя 13 21:45:13 localhost.localdomain httpd[5903]: Server configured, listening>
ноя 13 21:45:13 localhost.localdomain systemd[1]: Started The Apache HTTP Server>
...skipping...
● httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor pres>
  Active: active (running) since Sat 2021-11-13 21:45:13 MSK; 24s ago
    Docs: man:httpd.service(8)
 Main PID: 5903 (httpd)
   Status: "Running, listening on: port 81"
     Tasks: 213 (limit: 11252)
    Memory: 24.7M
      CGroup: /system.slice/httpd.service
              ├─5903 /usr/sbin/httpd -DFOREGROUND
              ├─5904 /usr/sbin/httpd -DFOREGROUND
              ├─5905 /usr/sbin/httpd -DFOREGROUND
              ├─5906 /usr/sbin/httpd -DFOREGROUND
              ├─5907 /usr/sbin/httpd -DFOREGROUND

ноя 13 21:45:13 localhost.localdomain systemd[1]: Stopped The Apache HTTP Server>
ноя 13 21:45:13 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 13 21:45:13 localhost.localdomain httpd[5903]: Server configured, listening>
ноя 13 21:45:13 localhost.localdomain systemd[1]: Started The Apache HTTP Server>
~
```

Figure 4.17: рис.19. Перезапуск сервера.

5. Проанализируем лог файлы. Проверим список портов и убедимся, что 81 появился в списке. Попробуем запустить сервер ещё раз. Успешно.(рис. 20-24)

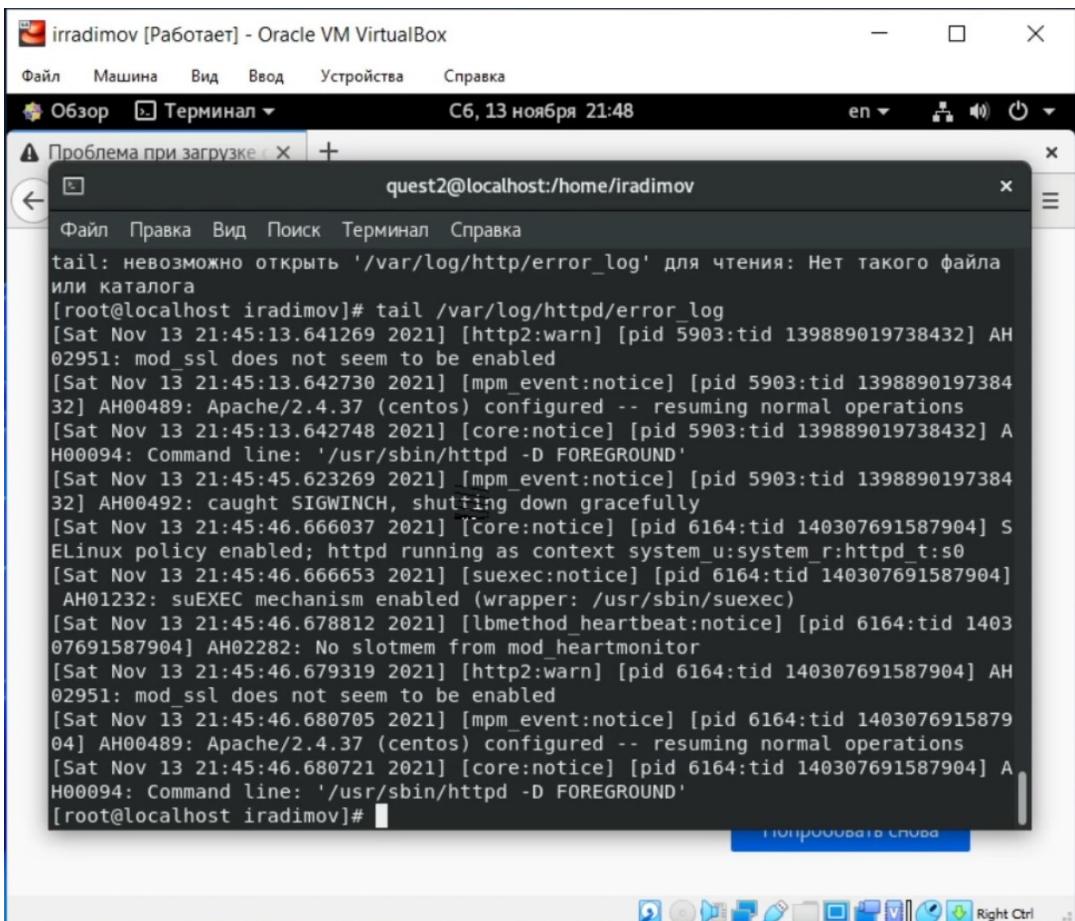


Figure 4.18: рис.20. Лог.

The screenshot shows a terminal window titled 'Terminál' with the command 'tail /var/log/audit/audit.log' running. The output displays several audit messages related to Apache HTTPD, indicating denied access attempts. The terminal window is part of a desktop environment with a menu bar at the top.

```
[root@localhost iradimov]# tail /var/log/audit/audit.log
type=AVC msg=audit(1636828730.202:245): avc: denied { setattr } for pid=3902
comm="httpd" path="/var/www/html/test.html" dev="dm-0" ino=34460232 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1636828730.202:245): arch=c000003e syscall=4 success=no e
xit=-13 a0=7f450803ba78 a1=7f4503ff6890 a2=7f4503ff6890 a3=7f4503ff74f0 items=0
ppid=3896 pid=3902 auid=4294967295 uid=48 gid=48 euid=48 suid=48 egid=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 AUID="unset" UID="apache" GID="apache" EUID="apache" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1636828730.202:245): proctitle=2F7573722F7362696E2F6874
747064002D44464F524547524F554E44
type=AVC msg=audit(1636828730.202:246): avc: denied { setattr } for pid=3902
comm="httpd" path="/var/www/html/test.html" dev="dm-0" ino=34460232 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1636828730.202:246): arch=c000003e syscall=6 success=no e
xit=-13 a0=7f450803bb58 a1=7f4503ff6890 a2=7f4503ff6890 a3=1 items=0 ppid=3896 p
id=3902 auid=4294967295 uid=48 gid=48 euid=48 suid=48 egid=48 sgid=48 f
sgid=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=lstat AUID="unset" UID="ap
ache" GID="apache" EUID="apache" SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
```

Figure 4.19: рис.21. Лог(часть2).

The screenshot shows a terminal window with the command 'semanage port -l | grep http_port_t' running. It lists two port ranges: 80, 81, 443, 488, 8008, 8009, 8443, 9000 and 5988. The terminal window is part of a desktop environment with a menu bar at the top.

```
[root@localhost iradimov]# 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@localhost iradimov]#
```

Figure 4.20: рис.23. Список портов.

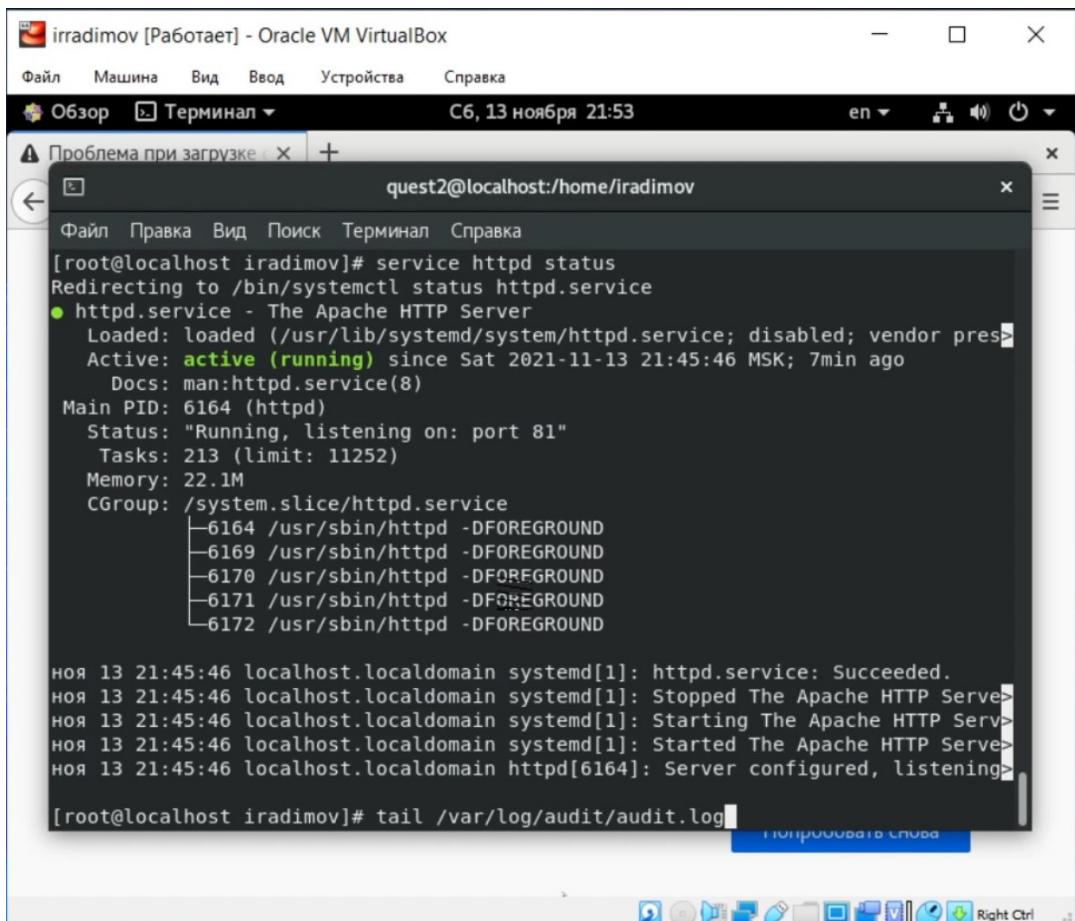


Figure 4.21: рис.24. Повторный перезапуск сервера.

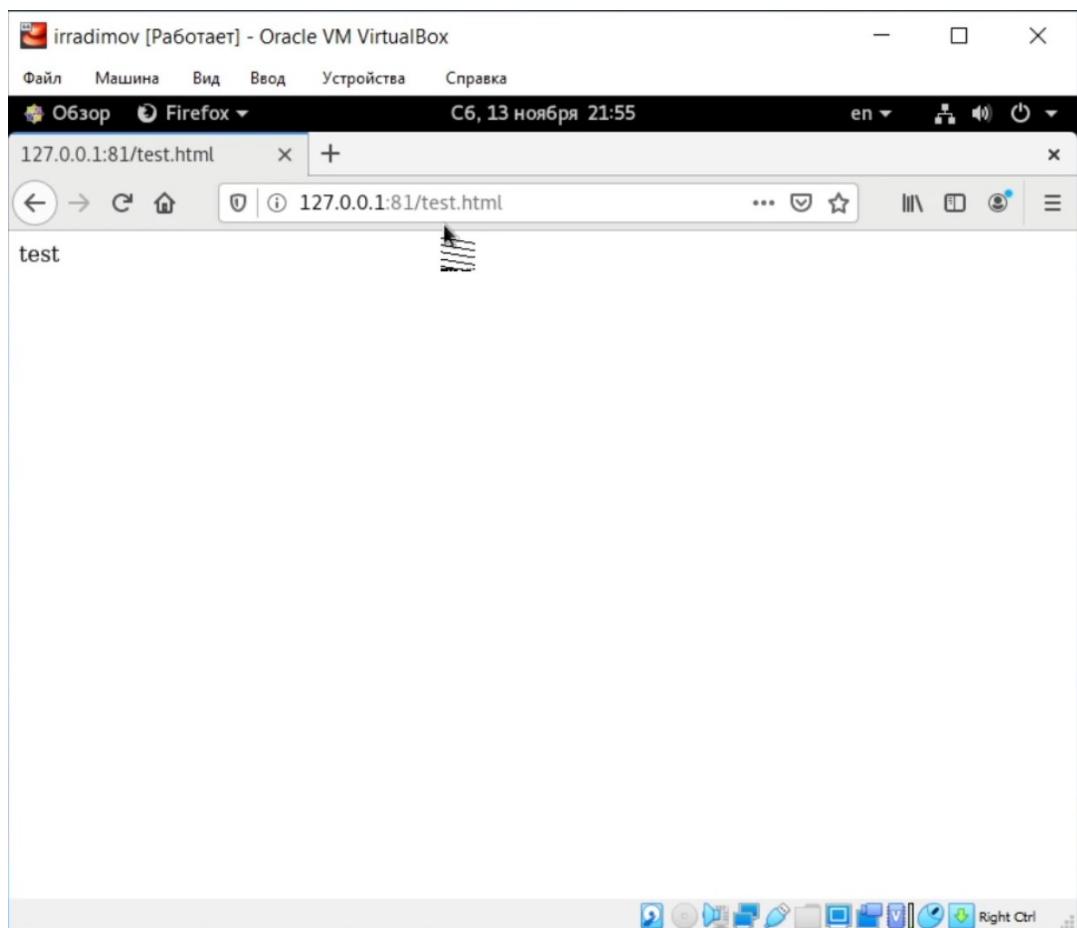


Figure 4.22: рис.24. Удачная попытка доступа к серверу.

6. Исправим обратно конфигурационный файл apache. Удалим привязку к 81 порту. Удалим файл test.html.(рис. 25-26)

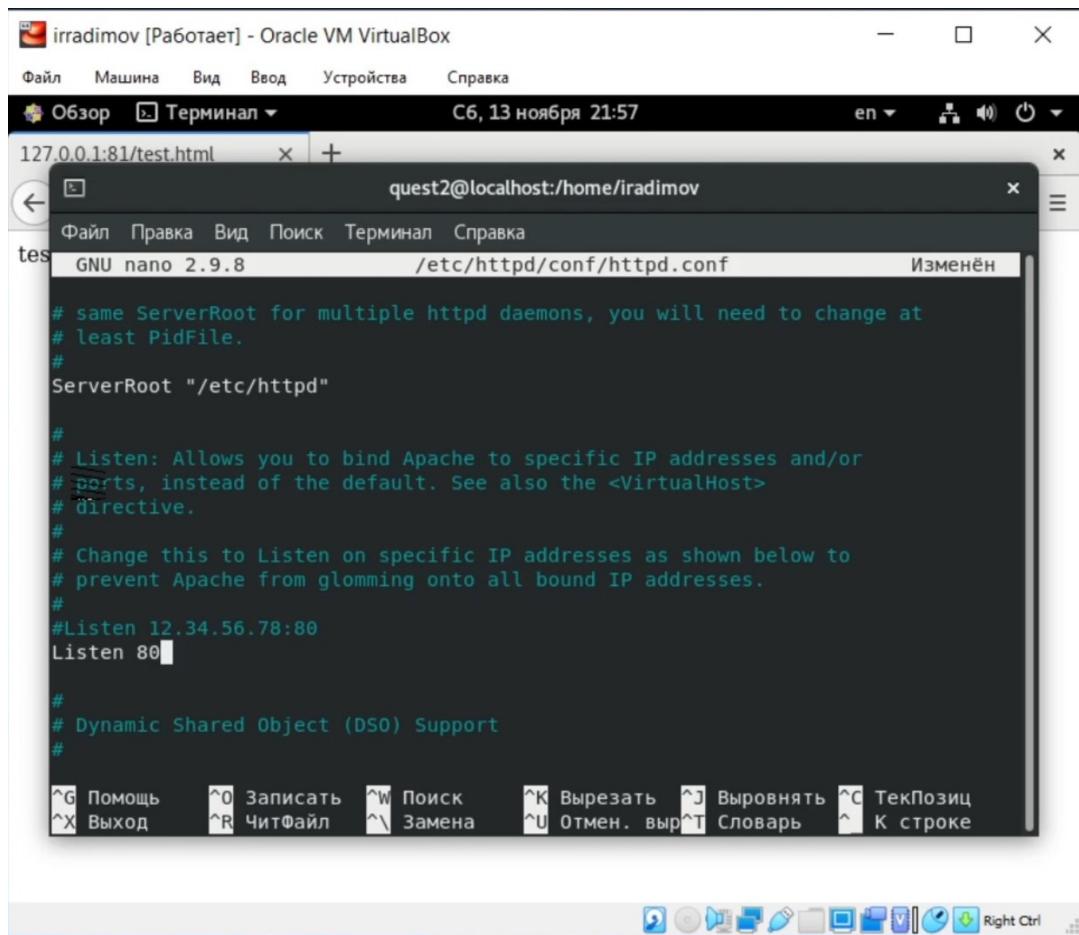


Figure 4.23: рис.25. Исправление конфигурационного файла.

The screenshot shows a terminal window titled 'quest2@localhost:/home/iradimov' running in Oracle VM VirtualBox. The terminal displays the following log output:

```
Tasks: 213 (limit: 11252)
Memory: 22.1M
CGroup: /system.slice/httpd.service
└─6164 /usr/sbin/httpd -DFOREGROUND
   ├─6169 /usr/sbin/httpd -DFOREGROUND
   ├─6170 /usr/sbin/httpd -DFOREGROUND
   ├─6171 /usr/sbin/httpd -DFOREGROUND
   └─6172 /usr/sbin/httpd -DFOREGROUND

ноя 13 21:45:46 localhost.localdomain systemd[1]: httpd.service: Succeeded.
ноя 13 21:45:46 localhost.localdomain systemd[1]: Stopped The Apache HTTP Server.
ноя 13 21:45:46 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 13 21:45:46 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
ноя 13 21:45:46 localhost.localdomain httpd[6164]: Server configured, listening...
```

Below the log, the terminal shows command history:

```
[root@localhost iradimov]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@localhost iradimov]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@localhost iradimov]# nano /etc/httpd/conf/httpd.conf
[root@localhost iradimov]# semanage port -d -t http_port_t -r tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@localhost iradimov]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@localhost iradimov]#
```

Figure 4.24: рис.26. Удаление привязки и файла.

5 Библиография

1. ТУИС РУДН

6 Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux1. Проверил работу SELinx на практике совместно с веб-сервером Apache.