

Отчет по лабораторной работе номер 6

Хамбалеев Булат Галимович

Содержание

1 Цель работы	5
2 Задание	6
3 Теория	7
4 Выполнение работы	8
5 Библиография	29
6 Выводы	30

List of Tables

List of Figures

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

1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux¹. Проверить работу SELinux на практике совместно с веб-сервером Apache.

2 Задание

Лабораторная работа подразумевает использование некоторых консольных команд для взаимодействия с кодом и веб-сервером.

3 Теория

Для запуска веб-сервера Apache нам понадобится установить пакет apache, доступный в официальных репозиториях. Затем настроить файл конфигурации, который находится по адресу /etc/httpd/conf. Для старта apache нужно запустить службу httpd.service.

4 Выполнение 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 1-4)

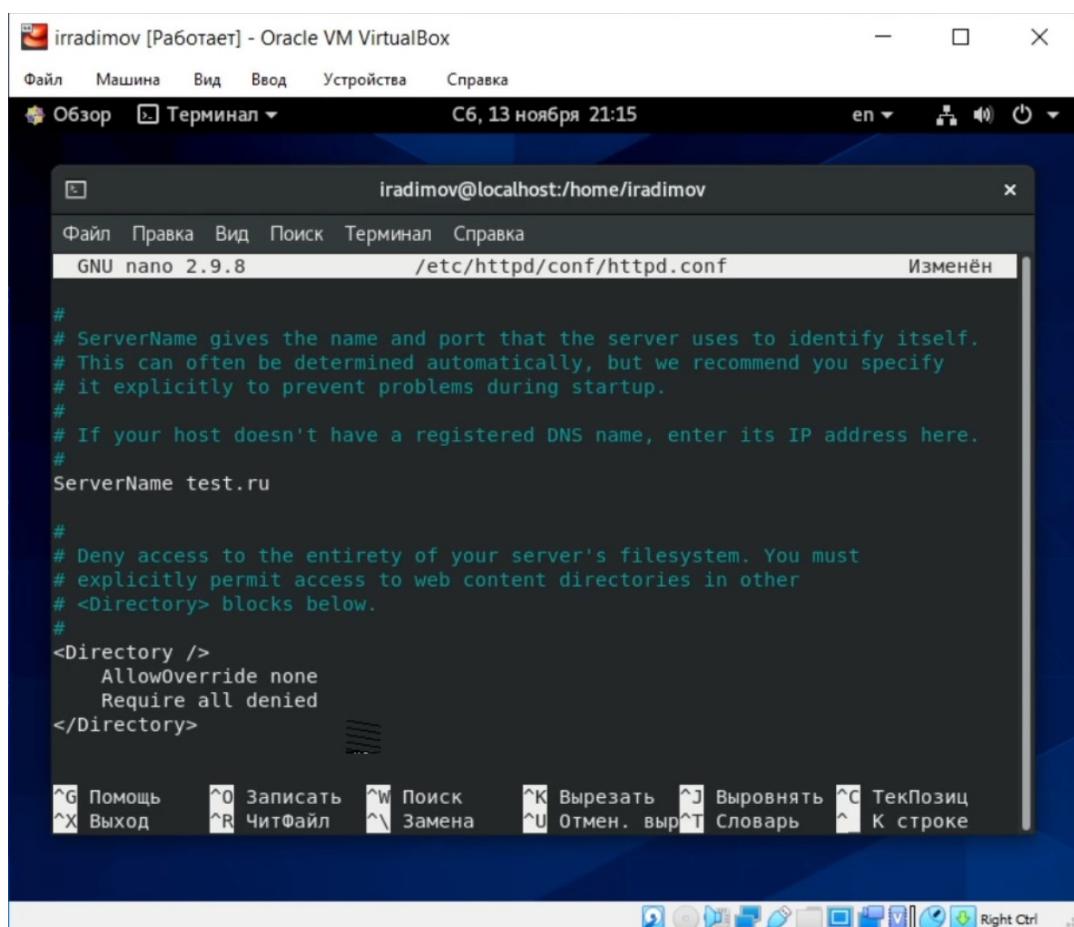
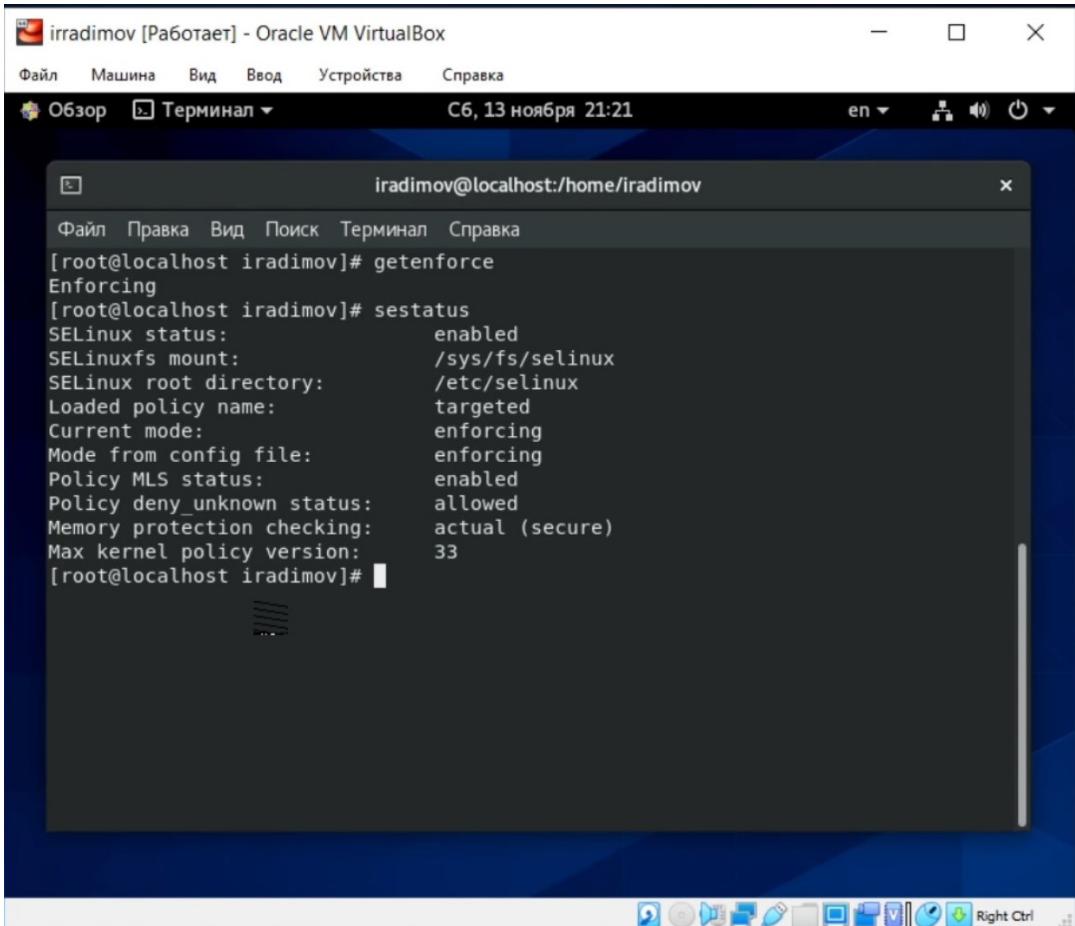


Figure 4.1: рис.1. Getenforce и sestatus.

```
[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 4.2: рис.2. Проверка работы веб-сервера.



The screenshot shows a terminal window titled "iradimov [Работает] - Oracle VM VirtualBox". The window contains the following command output:

```
Файл Правка Вид Поиск Терминал Справка
[root@localhost iradimov]# getenforce
Enforcing
[root@localhost iradimov]# 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
[root@localhost iradimov]#
```

Figure 4.3: рис.3. Список процессов.

```
[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

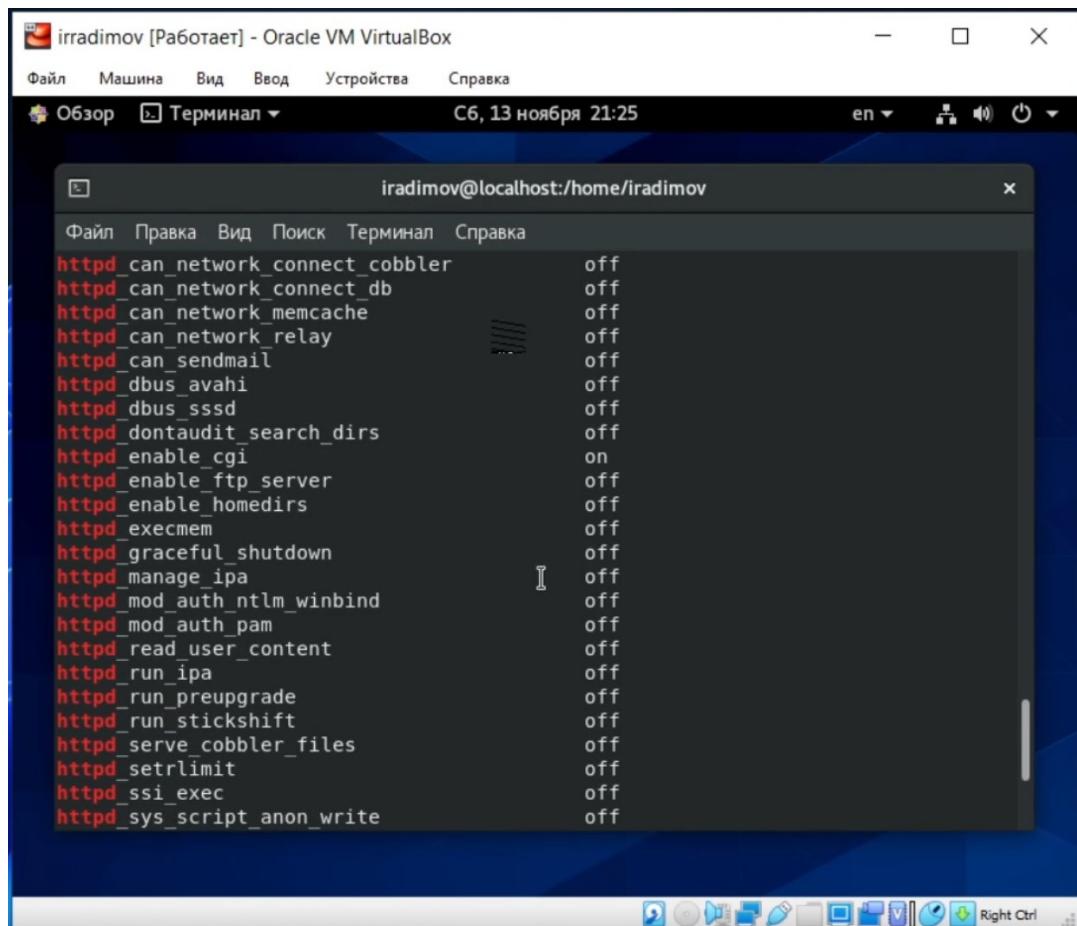
ноя 13 21:22:19 localhost.localdomain systemd[1]: Starting The Apache HTTP Serv>
ноя 13 21:22:19 localhost.localdomain systemd[1]: Started The Apache HTTP Serve>
ноя 13 21:22:19 localhost.localdomain httpd[3896]: Server configured, listening>
lines 1-18/18 (END)
```

Figure 4.4: рис.4. 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.5-8)

```
[root@localhost iradimov]# ps auxZ | grep httpd
system_u:system_r:httpt:s0    root      3896  0.0  0.5 273832 11024 ?
  Ss 21:22  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpt:s0    apache    3901  0.0  0.4 289836  8228 ?
  S 21:22  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpt:s0    apache    3902  0.0  0.5 1347644 9864 ?
  Sl 21:22  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpt:s0    apache    3903  0.0  0.5 1347644 9872 ?
  Sl 21:22  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpt: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 4.5: рис.5. Seinfo.



iradimov [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Обзор Терминал С6, 13 ноября 21:25 en

iradimov@localhost:/home/iradimov

```
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
httpd_graceful_shutdown off
httpd_manage_ipa off
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssi_exec off
httpd_sys_script_anon_write off
```

Figure 4.6: рис.6. Определение типа файлов и круга пользователей.

iradimov [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Обзор Терминал ▾ С6, 13 ноября 21:26 en ▾

iradimov@localhost:/home/iradimov

Файл Правка Вид Поиск Терминал Справка

```
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 4.7: рис.7. HTML код для веб сервера.

```
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 '/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 4.8: рис.8. 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.9-13)

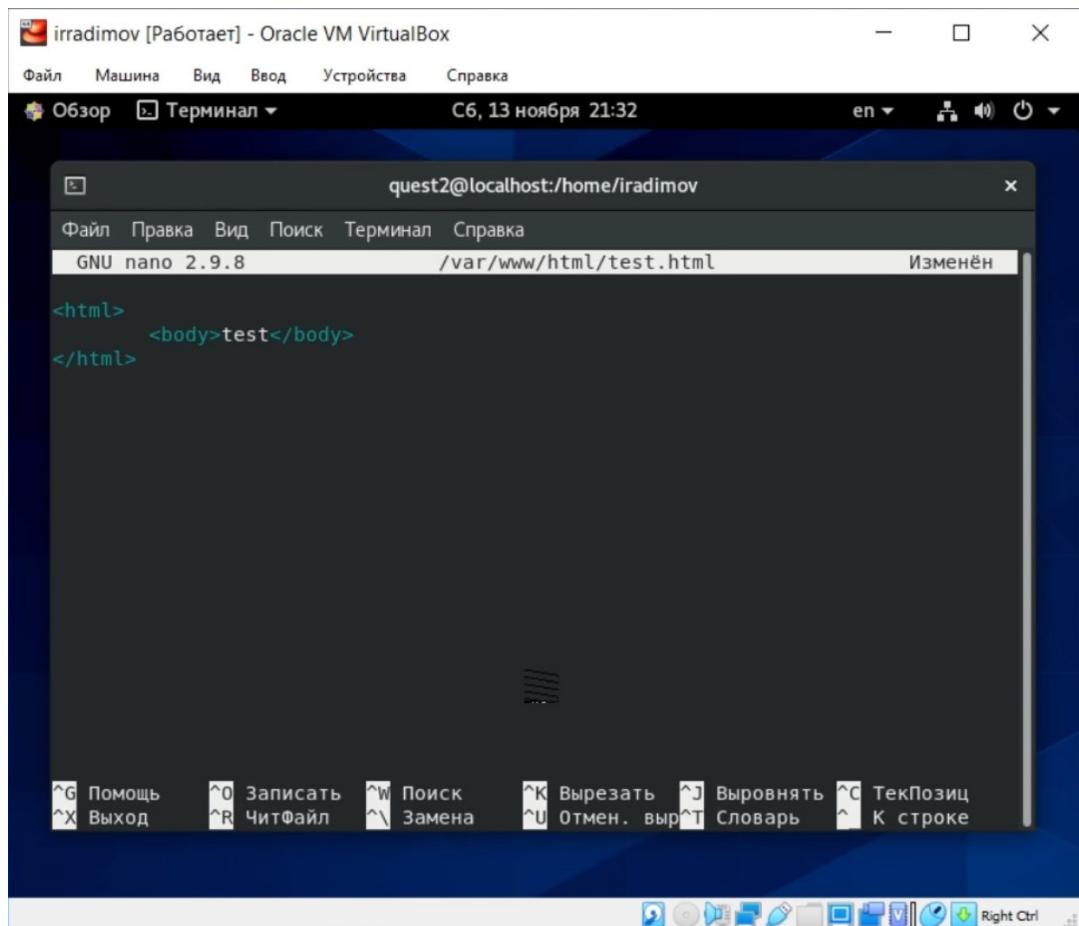
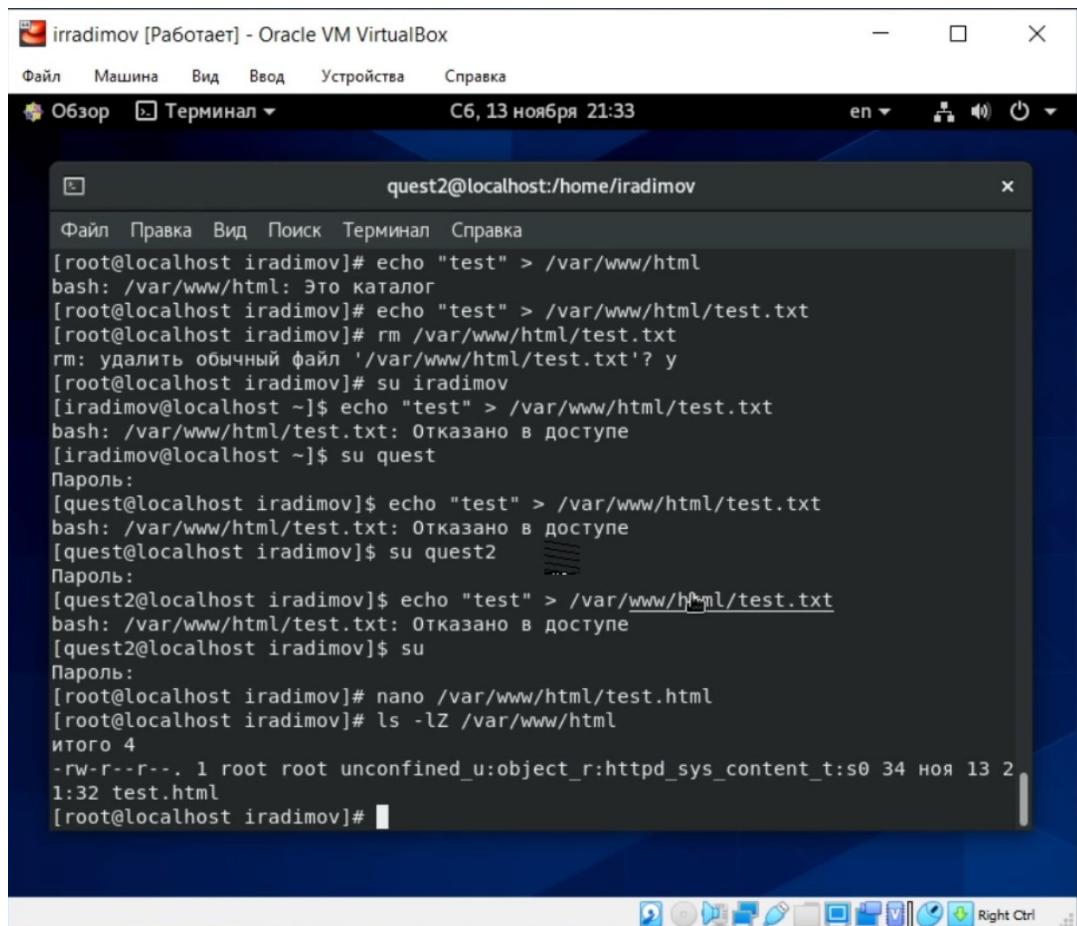


Figure 4.9: рис.9. Браузер и веб-сервер.



The screenshot shows a terminal window titled "quest2@localhost:/home/iradimov" running within an Oracle VM VirtualBox environment. The window title bar includes the machine name "iradimov [Работает]" and the application name "Oracle VM VirtualBox". The menu bar contains "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". The toolbar includes icons for "Обзор" and "Терминал". The status bar shows the date and time "Сб, 13 ноября 21:33" and language "en". The terminal window displays a command-line session where the user performs several actions:

```
[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 '/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
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 4.10: рис.10. Лог файлы.

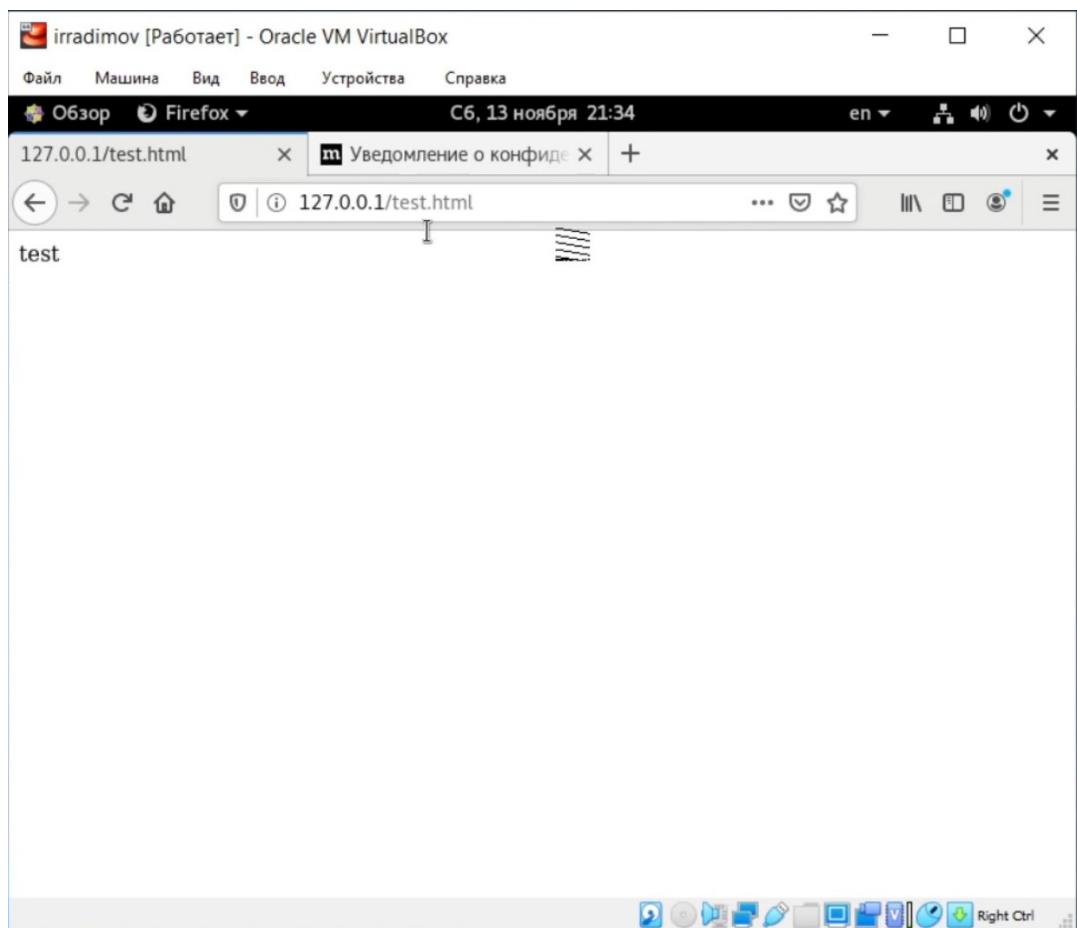
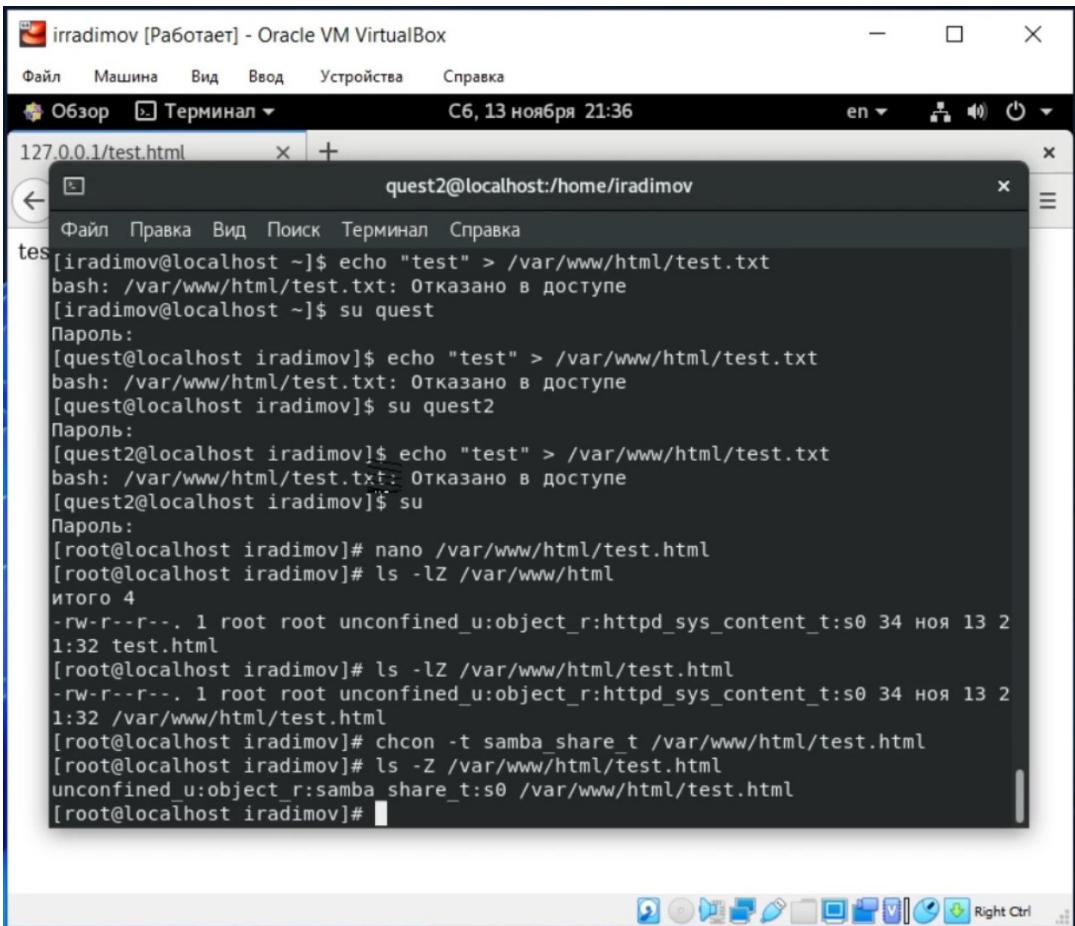


Figure 4.11: рис.11. Лог файлы(часть 2).



The screenshot shows a terminal window titled "quest2@localhost:/home/iradimov" running within an Oracle VM VirtualBox environment. The window title bar includes the machine name "iradimov [Работает]" and the date/time "С6, 13 ноября 21:36". The terminal interface has tabs for "Обзор" and "Терминал". The main pane displays the following command-line session:

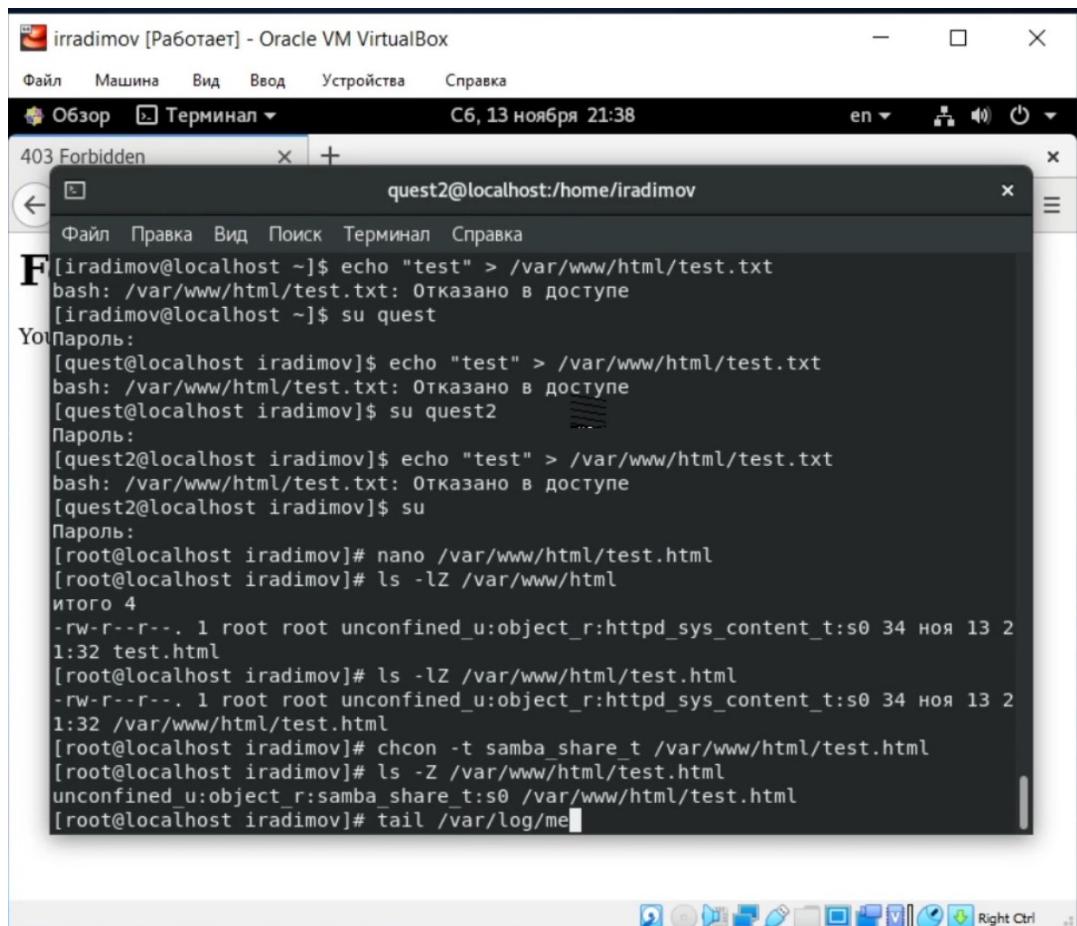
```
tes
[iradimov@localhost ~]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[iradimov@localhost ~]$ su quest
Пароль:
[quest@localhost iradimov]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[quest@localhost iradimov]$ 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 4.12: рис.12. Запрет доступа к веб-серверу.

```
[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]#
```

Figure 4.13: рис.13. Анализ ситуации.

4. Посмотрим лог файлы веб-сервера Apache. Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81. Выполним перезапуск(получен сбой). (рис.14-17)



The screenshot shows a terminal window titled "quest2@localhost:/home/iradimov" running within an Oracle VM VirtualBox environment. The terminal displays a log of commands and their results:

```
F [iradimov@localhost ~]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[iradimov@localhost ~]$ su quest
You have no privileges.
[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]# tail /var/log/me
```

Figure 4.14: рис.14. Лог веб-сервера.

The screenshot shows a terminal window titled "Terminál" (Terminal) in Russian, running on a Linux system. The window title bar includes "Обзор" (Overview), "Терминал" (Terminal), and "C6, 13 ноября 21:38". The menu bar has options like "Файл" (File), "Машина" (Machine), "Вид" (View), "Ввод" (Input), "Устройства" (Devices), and "Справка" (Help). The terminal window itself has tabs for "403 Forbidden" and "quest2@localhost:/home/iradimov". The current tab displays a root shell session with the following commands and output:

```
[iradimov@localhost ~]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[iradimov@localhost ~]$ su quest
You need to provide a password:
[quest@localhost iradimov]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[quest@localhost iradimov]$ su quest2
You need to provide a password:
[quest2@localhost iradimov]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[quest2@localhost iradimov]$ su
You need to provide a password:
[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 4.15: рис.15. Listen 81.

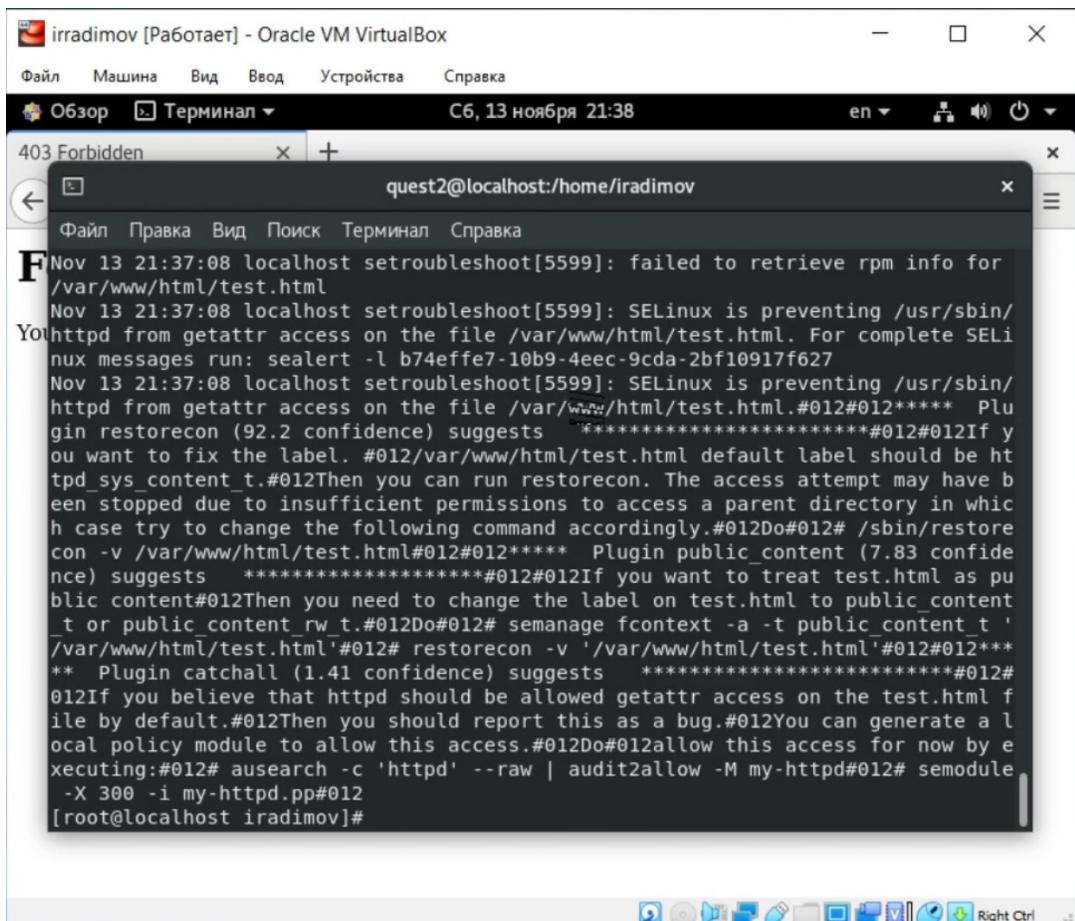


Figure 4.16: рис.16. Неудачная попытка соединения с веб-сервером через браузер.

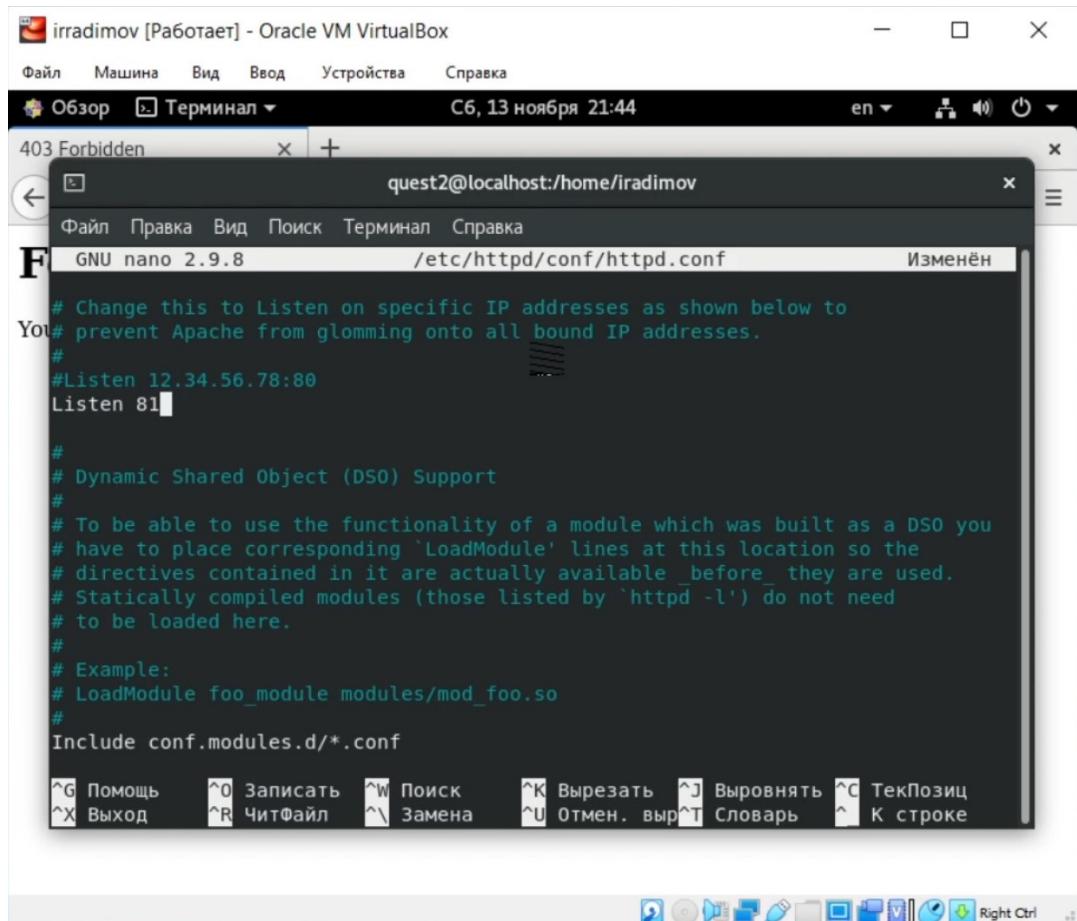


Figure 4.17: рис.17. Перезапуск сервера.

5. Проанализируем лог файлы. Проверим список портов и убедимся, что 81 появился в списке. Попробуем запустить сервер ещё раз. Успешно.(рис. 18-22)

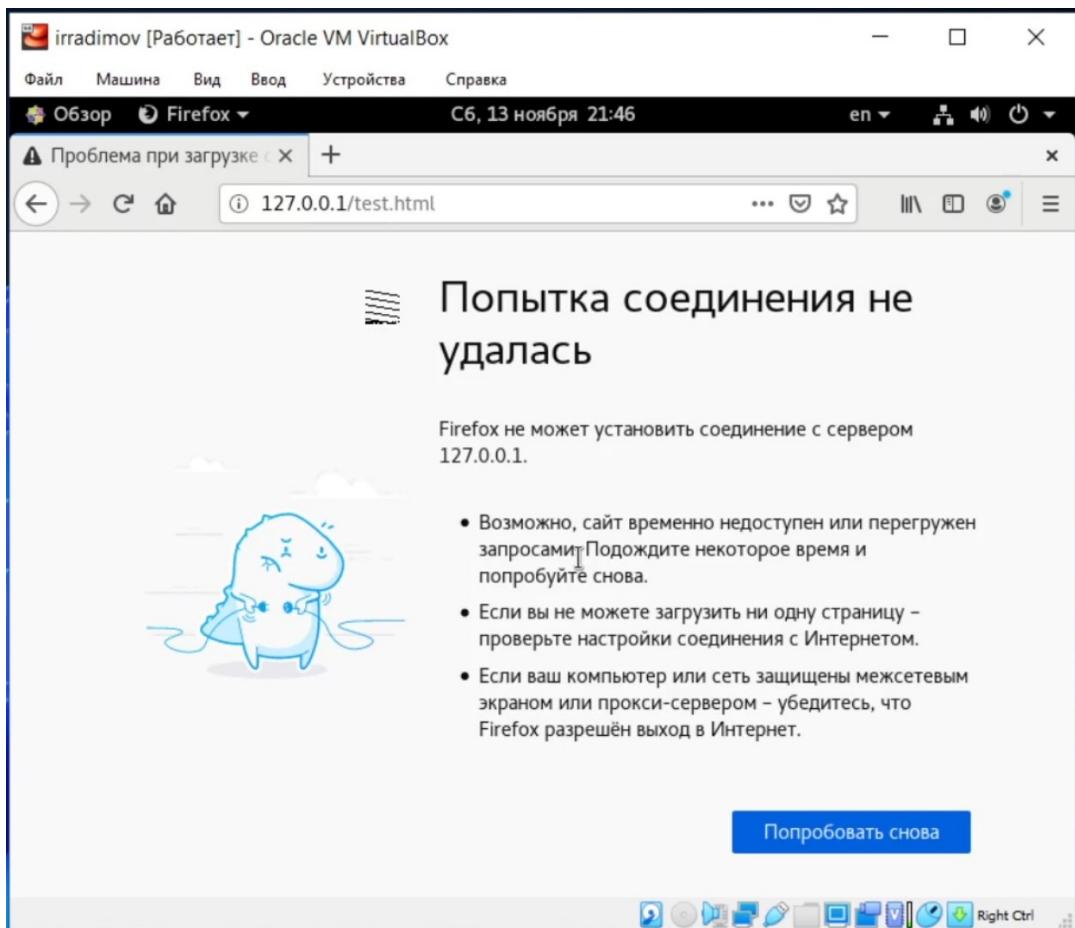
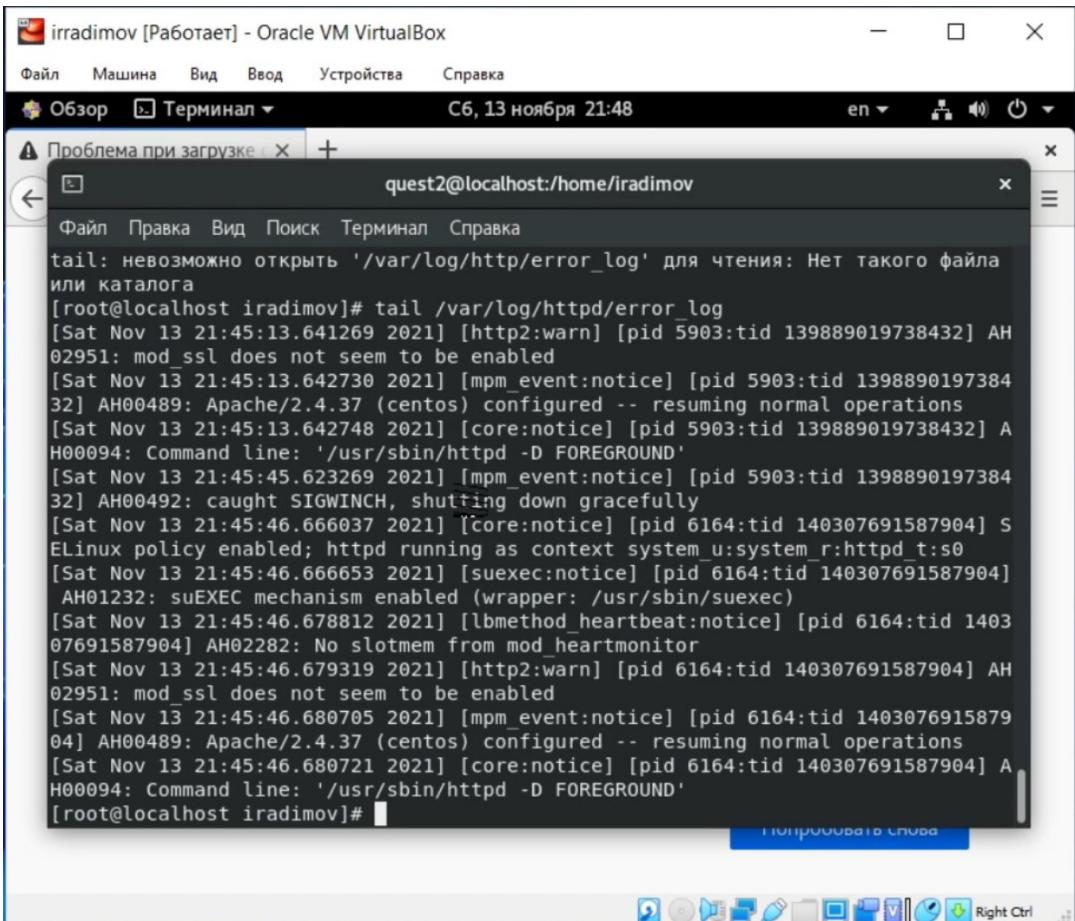


Figure 4.18: рис.18. Лог.

Figure 4.19: рис.19. Лог(часть2).



iradimov [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Обзор Терминал C6, 13 ноября 21:48 en

⚠ Проблема при загрузке + quest2@localhost:/home/iradimov

Файл Правка Вид Поиск Терминал Справка

```
tail: невозможно открыть '/var/log/http/error_log' для чтения: Нет такого файла или каталога
[root@localhost iradimov]# tail /var/log/httpd/error_log
[Sat Nov 13 21:45:13.641269 2021] [http2:warn] [pid 5903:tid 139889019738432] AH 02951: mod ssl does not seem to be enabled
[Sat Nov 13 21:45:13.642730 2021] [mpm_event:notice] [pid 5903:tid 139889019738432] AH00489: Apache/2.4.37 (centos) configured -- resuming normal operations
[Sat Nov 13 21:45:13.642748 2021] [core:notice] [pid 5903:tid 139889019738432] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Sat Nov 13 21:45:45.623269 2021] [mpm_event:notice] [pid 5903:tid 139889019738432] AH00492: caught SIGWINCH, shutting down gracefully
[Sat Nov 13 21:45:46.666037 2021] [core:notice] [pid 6164:tid 140307691587904] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Nov 13 21:45:46.666653 2021] [suexec:notice] [pid 6164:tid 140307691587904] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Nov 13 21:45:46.678812 2021] [lbmethod_heartbeat:notice] [pid 6164:tid 140307691587904] AH02282: No slotmem from mod_heartmonitor
[Sat Nov 13 21:45:46.679319 2021] [http2:warn] [pid 6164:tid 140307691587904] AH 02951: mod ssl does not seem to be enabled
[Sat Nov 13 21:45:46.680705 2021] [mpm_event:notice] [pid 6164:tid 140307691587904] AH00489: Apache/2.4.37 (centos) configured -- resuming normal operations
[Sat Nov 13 21:45:46.680721 2021] [core:notice] [pid 6164:tid 140307691587904] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[root@localhost iradimov]#
```

Figure 4.20: рис.20. Список портов.

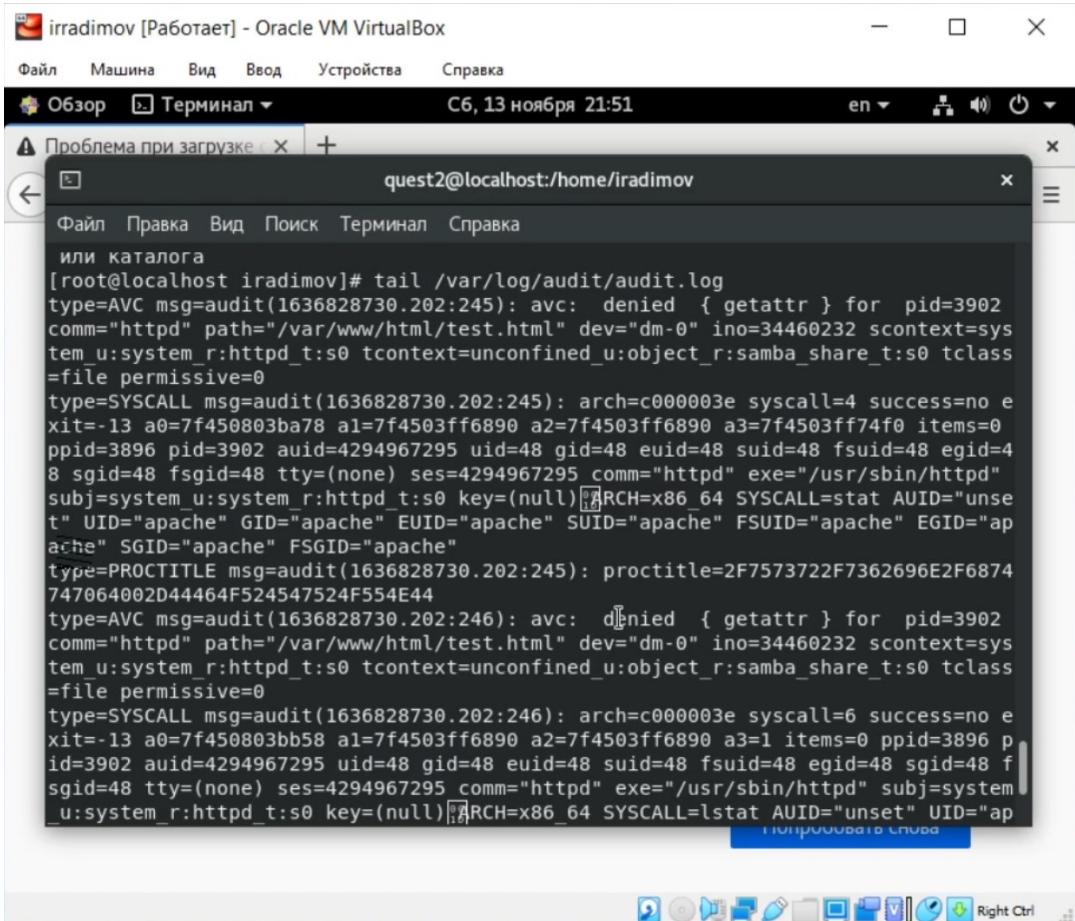


Figure 4.21: рис.21. Повторный перезапуск сервера.

```
[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]#
```

A screenshot of a terminal window showing the output of the 'semanage port -l | grep http_port_t' command. The output lists two ports: 80 and 8008, both associated with the 'http_port_t' type. This indicates that the Apache service is configured to listen on these ports.

Figure 4.22: рис.22. Удачная попытка доступа к серверу.

6. Исправим обратно конфигурационный файл apache. Удалим привязку к 81 порту. Удалим файл test.html.(рис. 23-27)

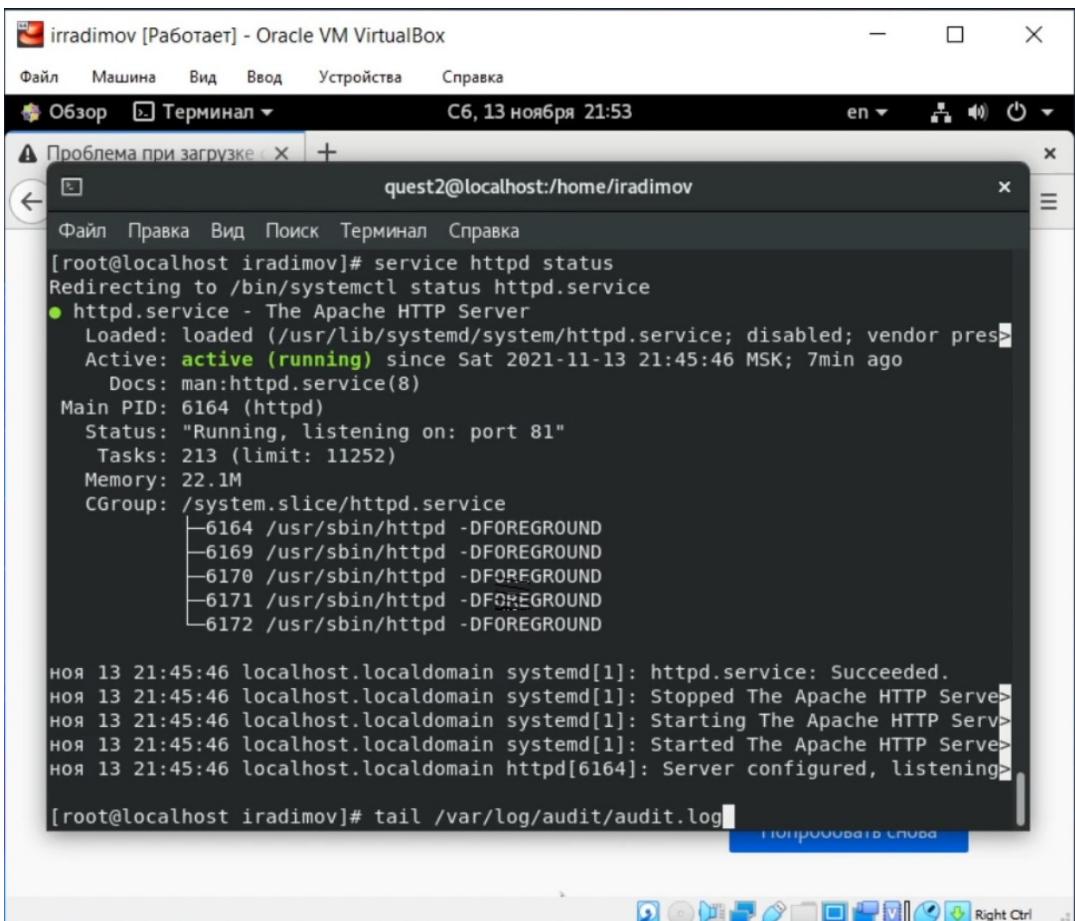


Figure 4.23: рис.23. Исправление конфигурационного файла.

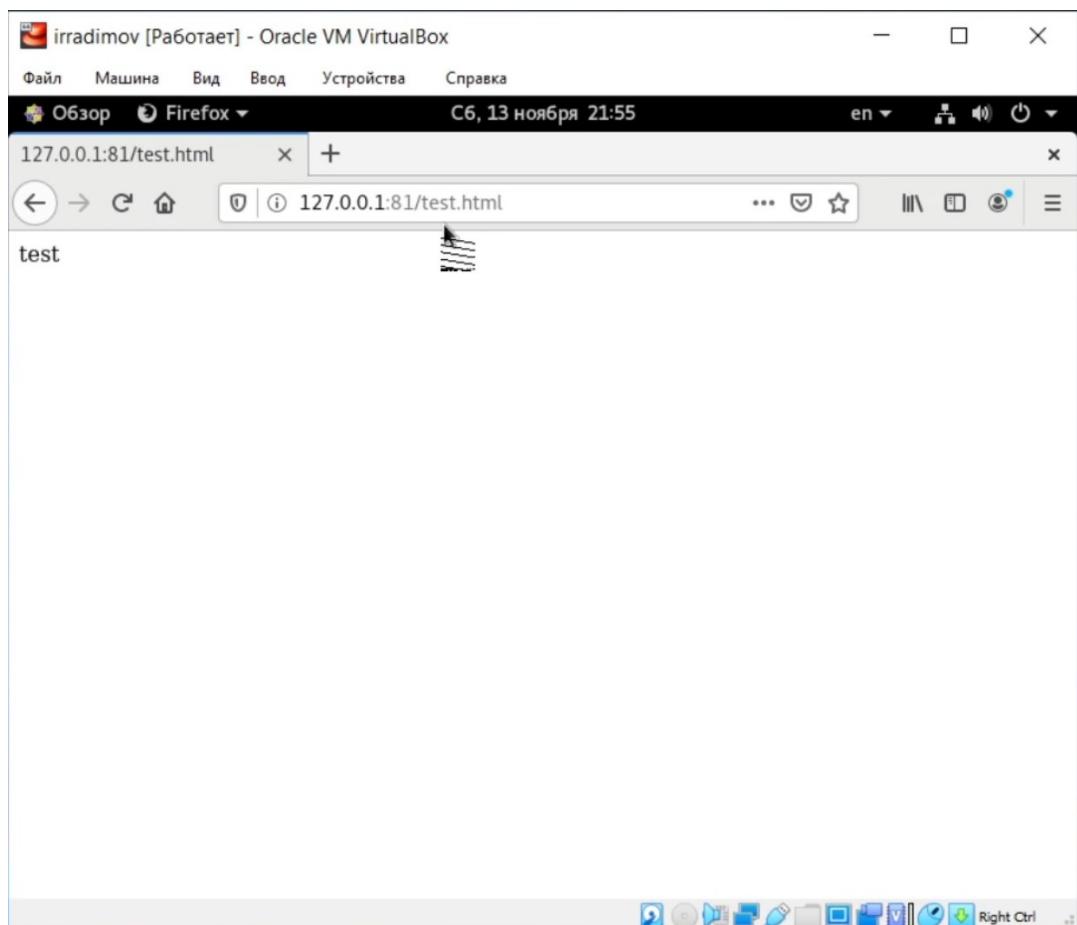


Figure 4.24: рис.24. Удаление привязки и файла.

5 Библиография

6 Выводы

Во время выполнения лабораторной работы я получил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.