

Отчёт по лабораторной работе 6

Мандатное разграничение прав в Linux

Гебриал Ибрам Есам Зекри НПИ-01-18

Содержание

1	Цель работы	5
2	Теоретические сведения	6
3	Выполнение лабораторной работы	8
4	Выводы	24
5	Список литературы	25

List of Tables

List of Figures

3.1	Проверка статус SELINUX	8
3.2	Установка параметра ServerName	9
3.3	Отключение фильтра	9
3.4	Проверка статуса	10
3.5	Запуск и проверка httpd	10
3.6	Контекст безопасности	11
3.7	Просмотр состояния переключателей SELinux для Apache	12
3.8	Просмотр статистики по политике с помощью команды seinfo	12
3.9	Определение типа файлов и поддиректорий, находящихся в директории /var/www	13
3.10	Создание html-файла и проверка его контекста	14
3.11	Содержание файла	14
3.12	Проверка html-файла в браузере	15
3.13	Изменение контекста файла /var/www/html/test.html и его проверка	15
3.14	Проверка html-файла в браузере	16
3.15	Анализ ситуации.	17
3.16	Проверка логи /var/log/messages	17
3.17	Замена порта прослушивание TCP	18
3.18	Выполнение перезапуска веб-сервера Apache	18
3.19	Анализ лог-файлы	19
3.20	Просмотр файла /var/log/http/error_log	19
3.21	Просмотр файла /var/log/http/access_log	19
3.22	Просмотр файла /var/log/audit/audit.log	20
3.23	Добавление порта 81 и проверка список портов	20
3.24	Попытка запуска веб-сервер Apache	21
3.25	Возвращение контекста файла	21
3.26	Попытка получения доступа к файлу через веб-сервер	22
3.27	Исправления обратно конфигурационный файл apache	22
3.28	Удаление привязки http_port_t к 81 порту и файла /var/www/html/test.html	23

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 Теоретические сведения

Linux с улучшенной безопасностью (SELinux) - это реализация мандатного управления доступом mandatory access control в ядре Linux, проверяющего разрешение операций после проверки стандартного дискреционного управления доступом discretionary access controls. SELinux создан Агентством Национальной Безопасности и вводит в действие правила для файлов и процессов в системе Linux, для совершаемых над ними действий, основываясь на установленной политике.

При использовании SELinux, файлы, включая директории и устройства являются объектами. Процессы, такие как, выполнение команды пользователем или приложение Mozilla® Firefox®, являются субъектами. Большинство операционных систем используют механизм дискретного контроля доступа (Discretionary Access Control (DAC)), который контролирует каким образом субъекты взаимодействуют с объектами, и как субъекты взаимодействуют друг с другом. В операционных системах с использованием DAC, пользователи контролируют права доступа к файлам (объектам), для которых они являются собственниками. Например, в операционных системах Linux®, пользователи могут сделать свои домашние директории читаемыми для всех, предоставив пользователям и процессам (субъектам) доступ к потенциально конфиденциальной информации, без какой либо защиты от этого нежелательных действий. [1]

Режимы работы SELinux

SELinux имеет три основных режим работы, при этом по умолчанию установлен режим Enforcing. Это довольно жесткий режим, и в случае необходимости он может быть изменен на более удобный для конечного пользователя.

Enforcing: Режим по-умолчанию. При выборе этого режима все действия, которые каким-то образом нарушают текущую политику безопасности, будут блокироваться, а попытка нарушения будет зафиксирована в журнале.

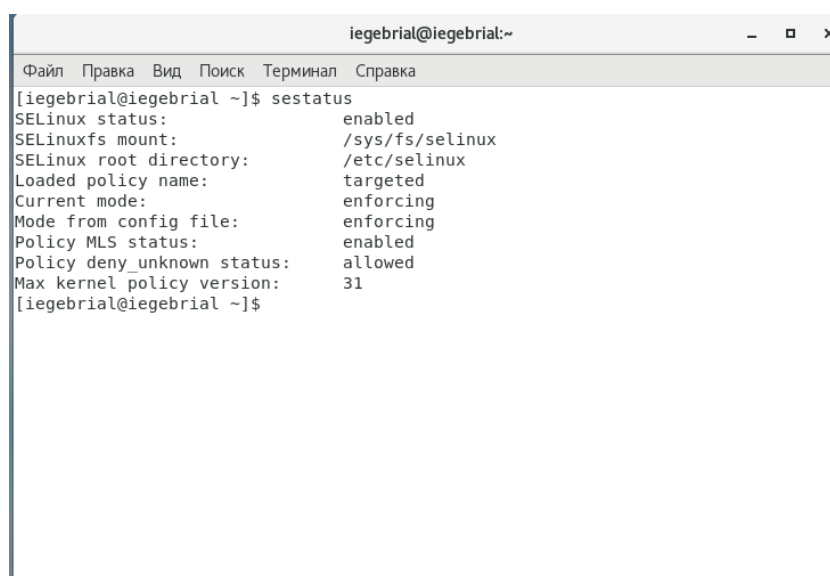
Permissive: В случае использования этого режима, информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы.

Disabled: Полное отключение системы принудительного контроля доступа.[2]

3 Выполнение лабораторной работы

Подготовка лабораторного стенда

1. При подготовке стенда обратил внимание, что необходимая для работы и указанная выше политика `targeted` и режим `enforcing` используются в данном дистрибутиве по умолчанию. (рис. 3.1)

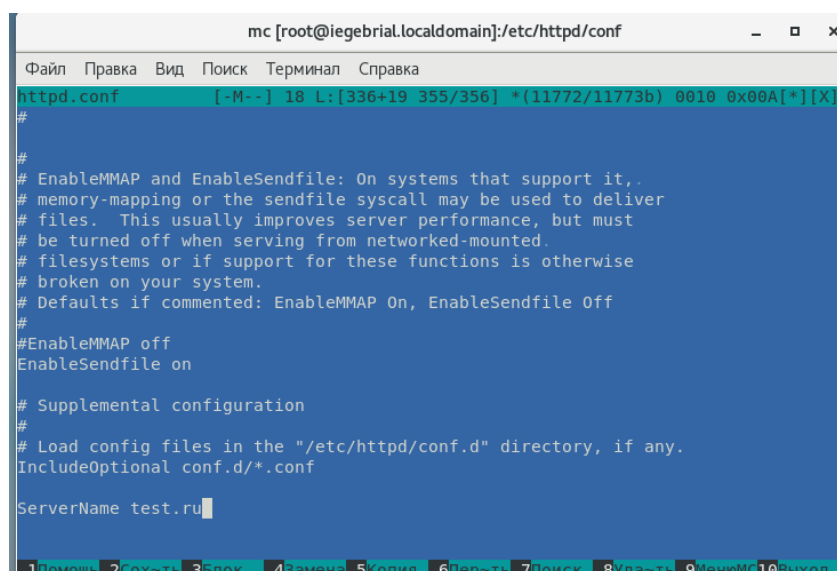


```
iegebrial@iegebrial:~  
Файл Правка Вид Поиск Терминал Справка  
[iegebrial@iegebrial ~]$ sestatus  
SELinux status: enabled  
SELinuxfs mount: /sys/fs/selinux  
SELinux root directory: /etc/selinux  
Loaded policy name: targeted  
Current mode: enforcing  
Mode from config file: enforcing  
Policy MLS status: enabled  
Policy deny_unknown status: allowed  
Max kernel policy version: 31  
[iegebrial@iegebrial ~]$
```

Figure 3.1: Проверка статус SELINUX

2. В конфигурационном файле `/etc/httpd/httpd.conf` задал параметр `ServerName`: (рис. 3.2)

Чтобы при запуске веб-сервера не выдавались лишние сообщения об ошибках, не относящихся к лабораторной работе.

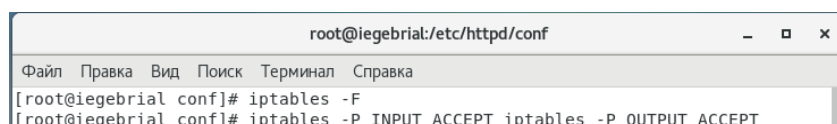


```
mc [root@iegebrial.localdomain]:/etc/httpd/conf
Файл  Правка  Вид  Поиск  Терминал  Справка
httpd.conf  [-M--] 18 L:[336+19 355/356] *(11772/11773b) 0010 0x00A[*][X]
#
#
# EnableMMAP and EnableSendfile: On systems that support it,.
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted.
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
#EnableSendfile on
#
# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
ServerName test.ru
```

Figure 3.2: Установка параметра ServerName

3. Также необходимо проследить, чтобы пакетный фильтр был отключён или в своей рабочей конфигурации позволял подключаться к 80-у и 81-у портам протокола tcp.

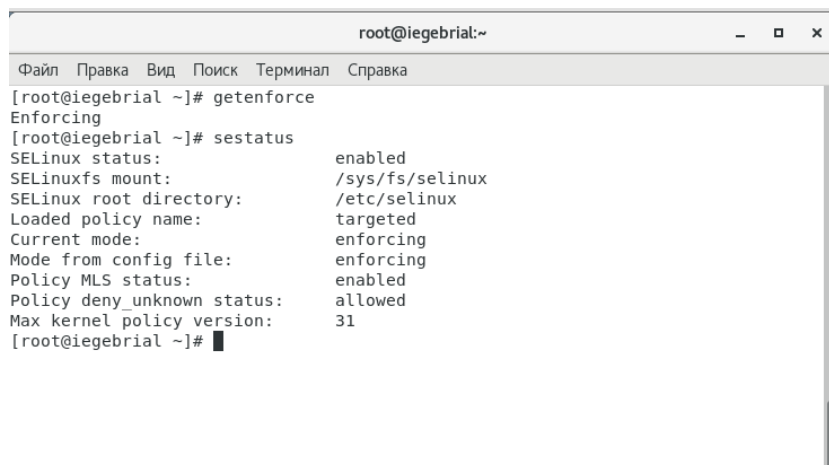
Отключил фильтр. (рис. 3.3)



```
root@iegebrial:/etc/httpd/conf
Файл  Правка  Вид  Поиск  Терминал  Справка
[root@iegebrial conf]# iptables -F
[root@iegebrial conf]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
```

Figure 3.3: Отключение фильтра

4. Вошёл в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. (рис. 3.4)

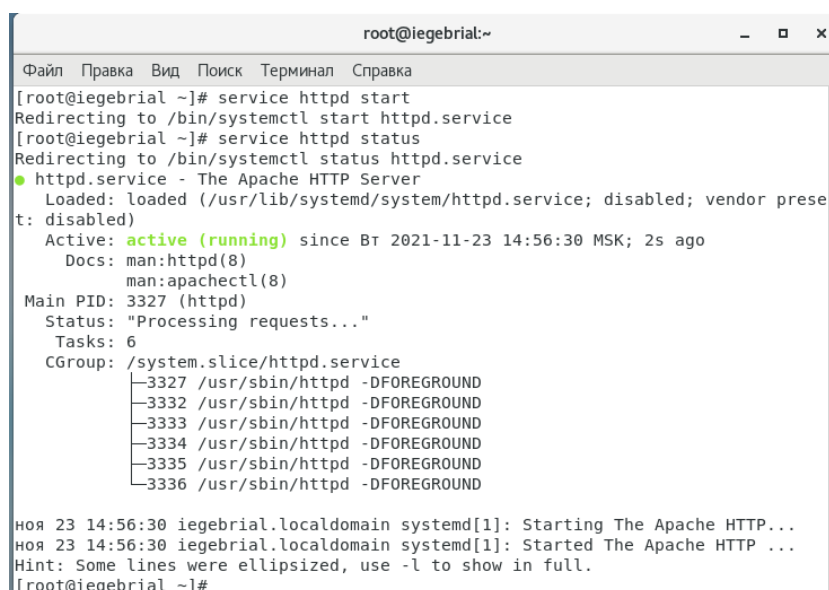
A terminal window titled 'root@iegebrial:~' with a menu bar containing 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows the following commands and output:

```
[root@iegebrial ~]# getenforce
Enforcing
[root@iegebrial ~]# 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
[root@iegebrial ~]#
```

Figure 3.4: Проверка статуса

5. Обратился с помощью браузера к веб-серверу, запущенному на своем компьютере, и убедился, что последний работает: (рис. 3.5)

Он не работал, поэтому запустил его так же, но с параметром start.

A terminal window titled 'root@iegebrial:~' with a menu bar containing 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows the following commands and output:

```
[root@iegebrial ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@iegebrial ~]# 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 prese
t: disabled)
   Active: active (running) since Вт 2021-11-23 14:56:30 MSK; 2s ago
     Docs: man:httpd(8)
           man:apachectl(8)
    Main PID: 3327 (httpd)
      Status: "Processing requests..."
        Tasks: 6
      CGroup: /system.slice/httpd.service
              └─3327 /usr/sbin/httpd -DFOREGROUND
                └─3332 /usr/sbin/httpd -DFOREGROUND
                  └─3333 /usr/sbin/httpd -DFOREGROUND
                    └─3334 /usr/sbin/httpd -DFOREGROUND
                      └─3335 /usr/sbin/httpd -DFOREGROUND
                        └─3336 /usr/sbin/httpd -DFOREGROUND

ноя 23 14:56:30 iegebrial.localdomain systemd[1]: Starting The Apache HTTP...
ноя 23 14:56:30 iegebrial.localdomain systemd[1]: Started The Apache HTTP ...
Hint: Some lines were ellipsized, use -l to show in full.
[root@iegebrial ~]#
```

Figure 3.5: Запуск и проверка httpd

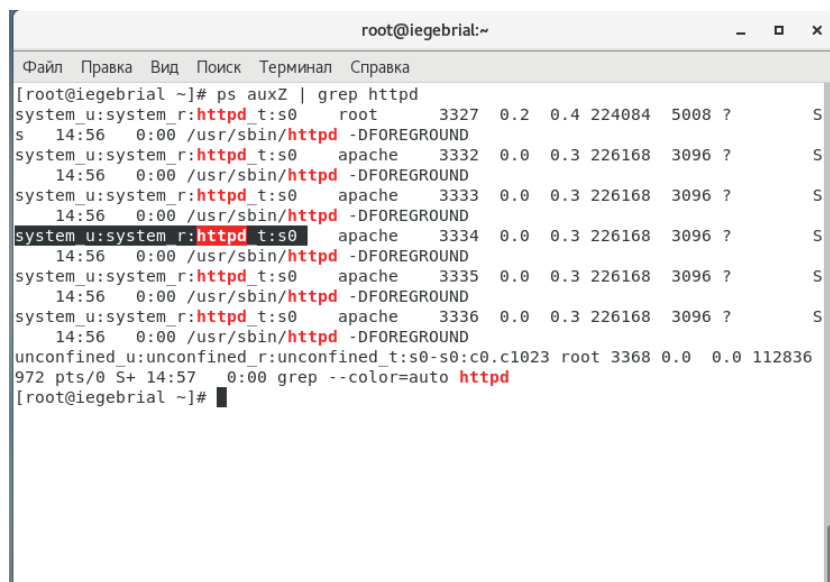
6. Нашёл веб-сервер Apache в списке процессов, определил его контекст безопасности. (рис. 3.6)

system_u — системный пользователь;

system_r — роль уровня системы, используемая для запуска системных процессов с указанием конкретного типа субъекта, определяемого типом объекта (файла).

httpd_t- задан тип

s0- задан уровень



```
root@iegebrial:~  
Файл Правка Вид Поиск Терминал Справка  
[root@iegebrial ~]# ps auxZ | grep httpd  
system_u:system_r:httpd_t:s0 root 3327 0.2 0.4 224084 5008 ? S  
s 14:56 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3332 0.0 0.3 226168 3096 ? S  
14:56 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3333 0.0 0.3 226168 3096 ? S  
14:56 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3334 0.0 0.3 226168 3096 ? S  
14:56 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3335 0.0 0.3 226168 3096 ? S  
14:56 0:00 /usr/sbin/httpd -DFOREGROUND  
system_u:system_r:httpd_t:s0 apache 3336 0.0 0.3 226168 3096 ? S  
14:56 0:00 /usr/sbin/httpd -DFOREGROUND  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 3368 0.0 0.0 112836  
972 pts/0 S+ 14:57 0:00 grep --color=auto httpd  
[root@iegebrial ~]#
```

Figure 3.6: Контекст безопасности

7. Посмотрел текущее состояние переключателей SELinux для Apache. (рис. 3.7)

Можем заметить, что многие из них находятся в положении «off»

```
root@iegebrial:~  
Файл Правка Вид Поиск Терминал Справка  
[root@iegebrial ~]# sestatus -b httpd  
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  
  
Policy booleans:  
abrt_anon_write off  
abrt_handle_event off  
abrt_upload_watch_anon_write on  
antivirus_can_scan_system off  
antivirus_use_jit off  
auditadm_exec_content on  
authlogin_nsswitch_use_ldap off  
authlogin_radius off  
authlogin_yubikey off  
awstats_purge_apache_log_files off  
boinc_execmem on  
cdrecord_read_content off  
cluster_can_network_connect off  
cluster_manage_all_files off  
cluster_use_execmem off
```

Figure 3.7: Просмотр состояния переключателей SELinux для Apache

8. Посмотрел статистику по политике с помощью команды seinfo (рис. 3.8)

пользователей 8


ролей 14

типов 4793

```
root@iegebrial:~  
Файл Правка Вид Поиск Терминал Справка  
[root@iegebrial ~]# seinfo  
  
Statistics for policy file: /sys/fs/selinux/policy  
Policy Version & Type: v.31 (binary, mls)  
  
Classes: 130 Permissions: 272  
Sensitivities: 1 Categories: 1024  
Types: 4793 Attributes: 253  
Users: 8 Roles: 14  
Booleans: 316 Cond. Expr.: 362  
Allow: 107834 Neverallow: 0  
Auditallow: 158 Dontaudit: 10022  
Type_trans: 18153 Type_change: 74  
Type_member: 35 Role_allow: 37  
Role_trans: 414 Range_trans: 5899  
Constraints: 143 Validatetrans: 0  
Initial SIDs: 27 Fs_use: 32  
Genfscon: 103 Portcon: 614  
Netifcon: 0 Nodecon: 0  
Permissives: 0 Polcap: 5  
  
[root@iegebrial ~]#
```

Figure 3.8: Просмотр статистики по политике с помощью команды seinfo

9. Определил тип файлов и поддиректорий, находящихся в директории /var/www (рис. 3.9)



```
root@iegebrial:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[root@iegebrial ~]# 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  
[root@iegebrial ~]#
```

Figure 3.9: Определение типа файлов и поддиректорий, находящихся в директории /var/www

10. Создал от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html следующего содержания и проверял его конескст. (рис. 3.10) (рис. 3.11)

unconfined_u — прочие пользователи;

object_r — роль, указываемая для объектов типа файл или каталог;

httpd_sys_content_t- тип

s0- уровень.



Figure 3.12: Проверка html-файла в браузере

12. Изменил контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`: (рис. 3.13)

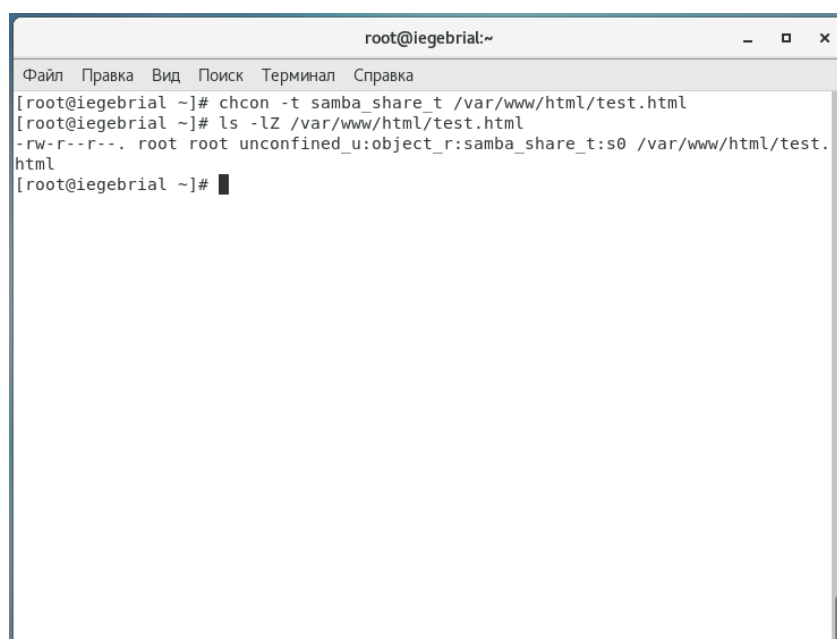


Figure 3.13: Изменение контекста файла `/var/www/html/test.html` и его проверка

13. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в

браузере адрес `http://127.0.0.1/test.html`. (рис. 3.14)

Получил сообщение об ошибке: `Forbidden You don't have permission to access /test.html on this server.`

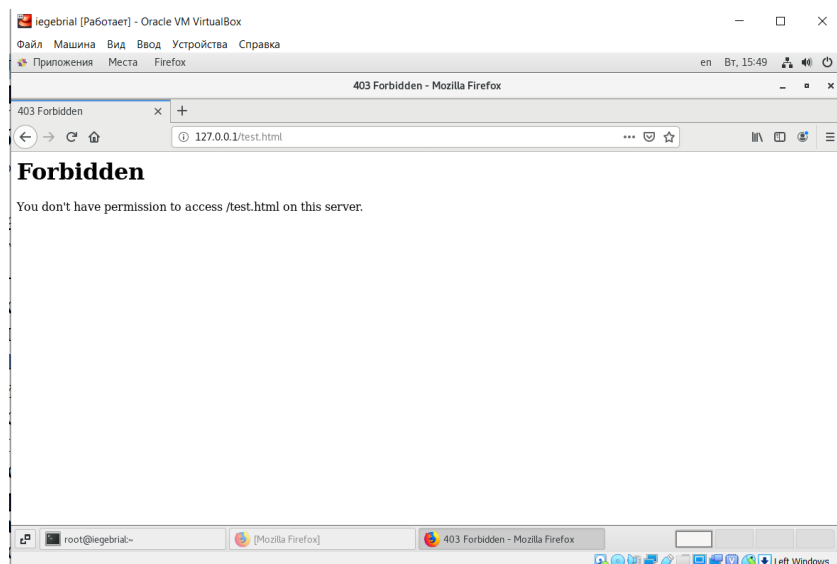


Figure 3.14: Проверка html-файла в браузере

14. Проанализировал ситуацию. (рис. 3.15) и просмотрел log-файлы веб-сервера Apache(рис. 3.16)

Заметил что не отображен потому что у `httpd` не доступа к типу файла. `SELinux` запретил доступ из за разницы в контекстах.

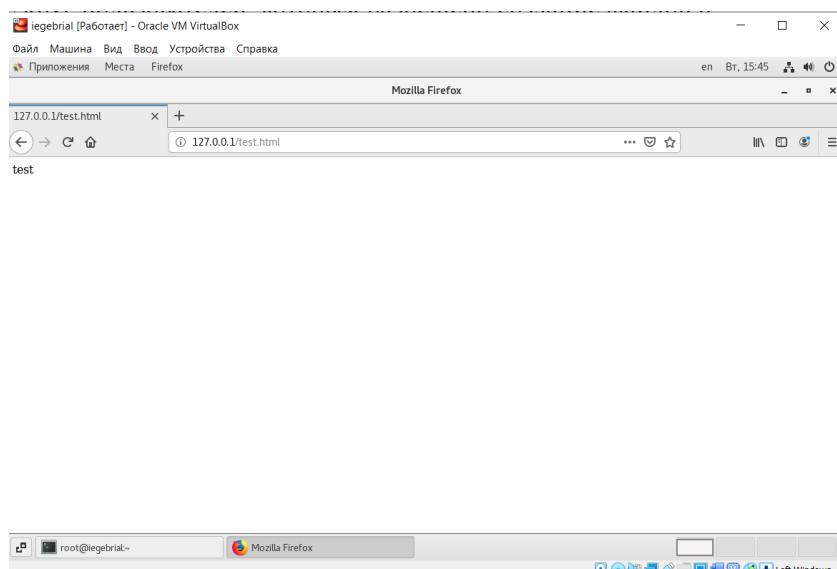


Figure 3.15: Анализ ситуации.

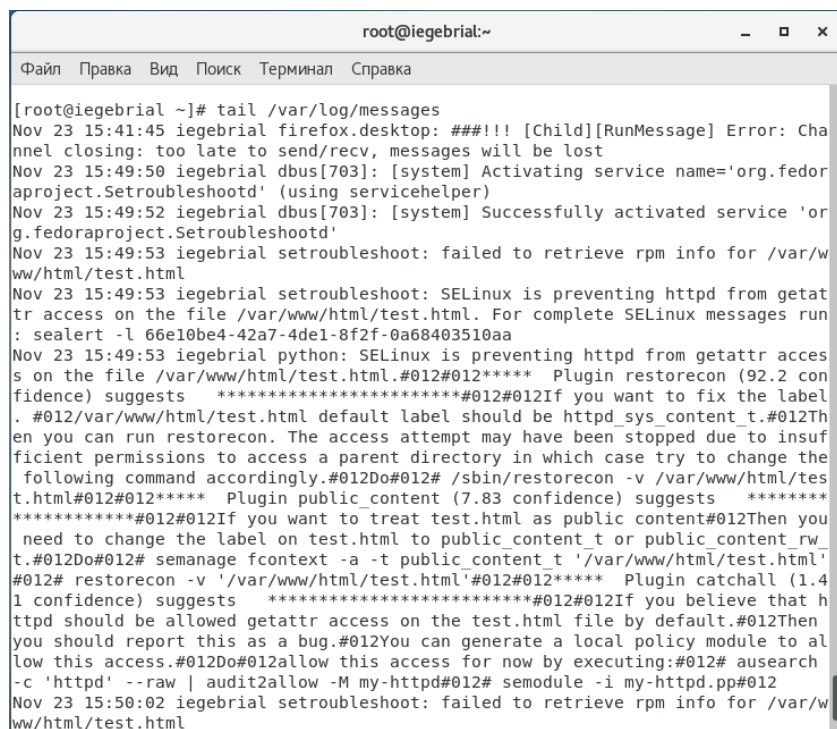
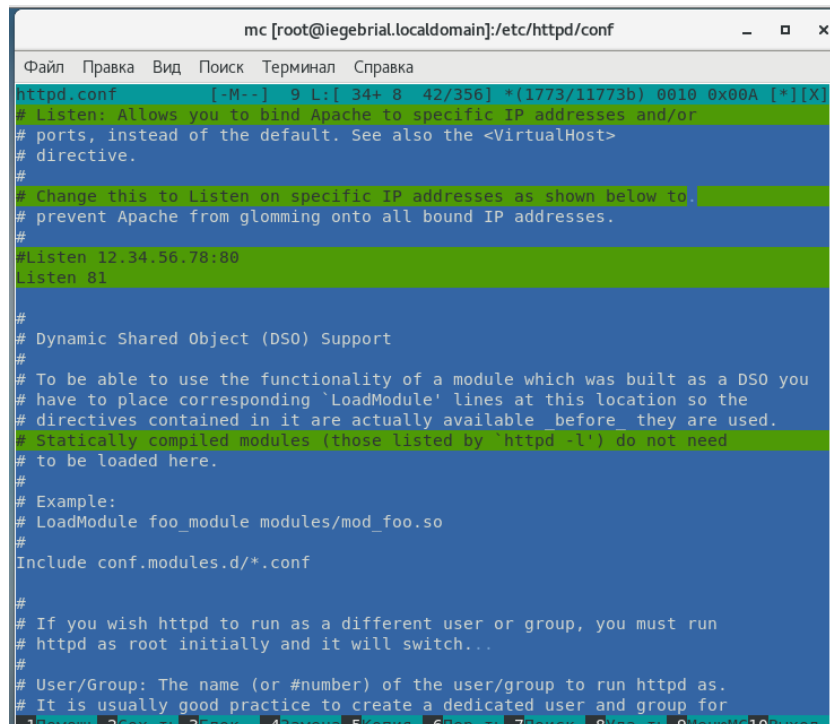


Figure 3.16: Проверка логи /var/log/messages

15. Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf нашёл строчку Listen 80 и заменил её на Listen

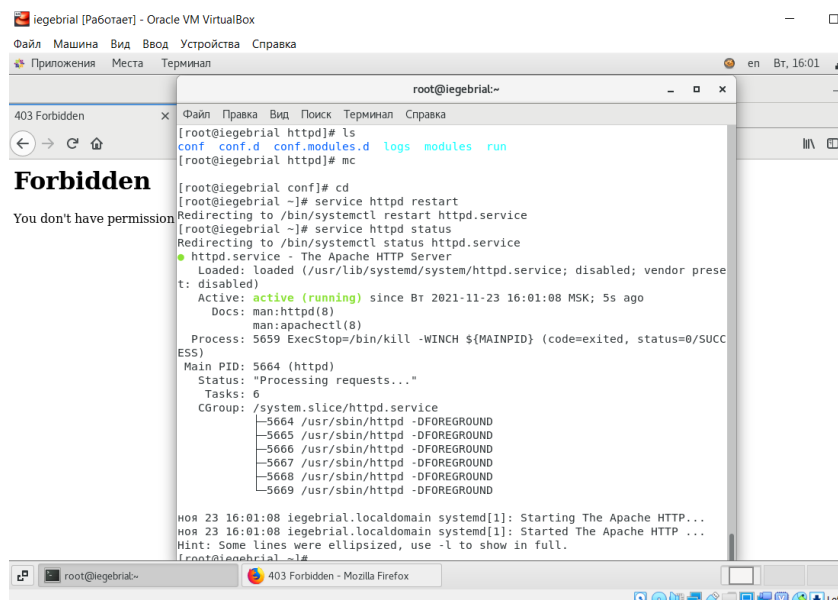
81. (рис. 3.17)



```
mc [root@iegebrial.localdomain]:/etc/httpd/conf
Файл Правка Вид Поиск Терминал Справка
httpd.conf [-M--] 9 L: [ 34+ 8 42/356] *(1773/11773b) 0010 0x00A [*][X]
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 81
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available before they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/*.conf
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch...
#
# User/Group: The name (or #number) of the user/group to run httpd as.
# It is usually good practice to create a dedicated user and group for
```

Figure 3.17: Замена порта прослушивание TCP

16. Выполнил перезапуск веб-сервера Apache. (рис. 3.18)



```
root@iegebrial:~
[root@iegebrial httpd]# ls
conf conf.d conf.modules.d logs modules run
[root@iegebrial httpd]# mc
[root@iegebrial conf]# cd
[root@iegebrial ~]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@iegebrial ~]# 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 prese
t: disabled)
   Active: active (running) since Вт 2021-11-23 16:01:08 MSK; 5s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 5659 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCC
ESS)
    Main PID: 5664 (httpd)
      Status: "Processing requests..."
        Tasks: 6
      CGroup: /system.slice/httpd.service
              └─5664 /usr/sbin/httpd -DFOREGROUND
                └─5665 /usr/sbin/httpd -DFOREGROUND
                  └─5666 /usr/sbin/httpd -DFOREGROUND
                    └─5667 /usr/sbin/httpd -DFOREGROUND
                      └─5668 /usr/sbin/httpd -DFOREGROUND
                        └─5669 /usr/sbin/httpd -DFOREGROUND

ноя 23 16:01:08 iegebrial.localdomain systemd[1]: Starting The Apache HTTP...
ноя 23 16:01:08 iegebrial.localdomain systemd[1]: Started The Apache HTTP ...
Hint: Some lines were ellipsized, use -l to show in full.
[root@iegebrial ~]#
```

Figure 3.18: Выполнение перезапуска веб-сервера Apache

17. Проанализировал лог-файлы: (рис. 3.19)

Мы можем видеть что нет ошибок.

```
[root@iegebrial ~]# tail -n1 /var/log/messages
Nov 23 16:01:08 iegebrial systemd: Started The Apache HTTP Server.
[root@iegebrial ~]# cat /var/log/http/error_log
```

Figure 3.19: Анализ лог-файлы

18. Просмотрел файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log (рис. 3.20)(рис. 3.21)(рис. 3.22)

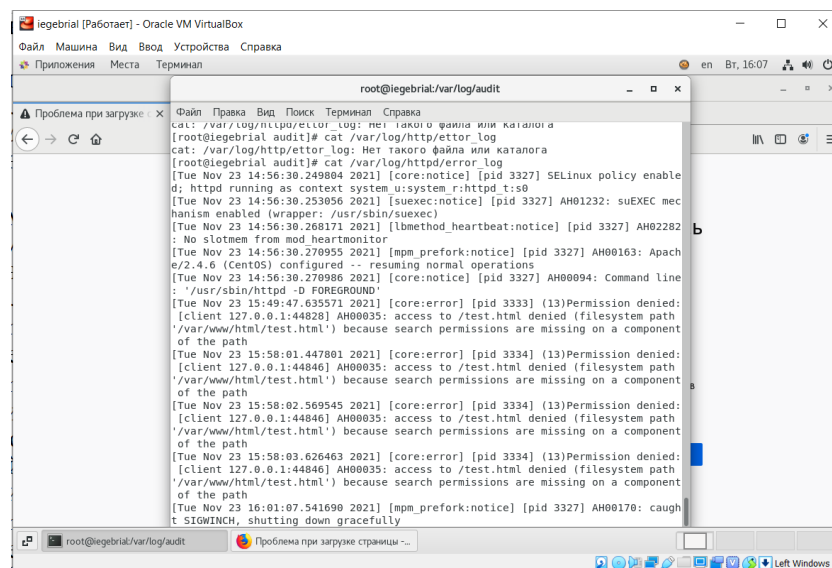


Figure 3.20: Просмотр файла /var/log/http/error_log

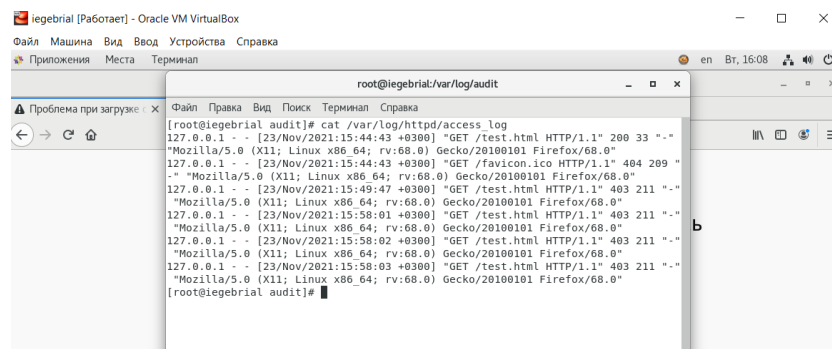


Figure 3.21: Просмотр файла /var/log/http/access_log

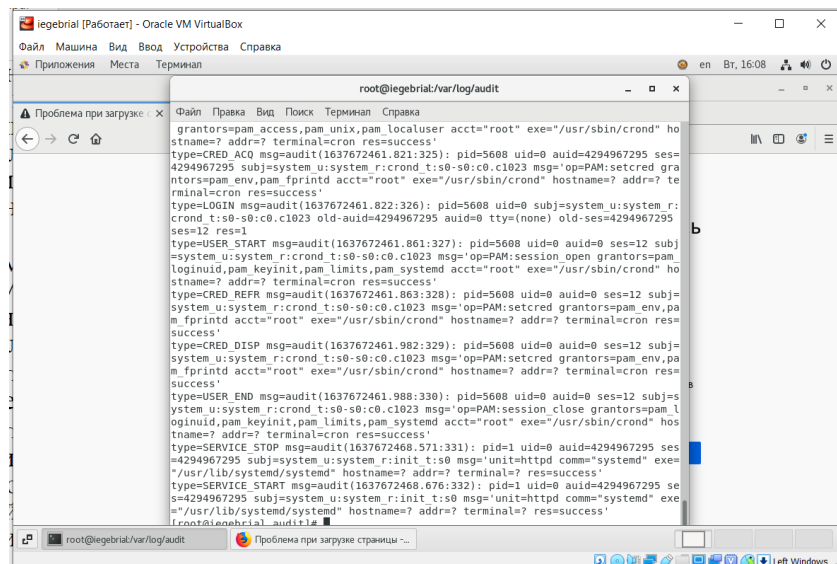


Figure 3.22: Просмотр файла /var/log/audit/audit.log

19. Выполнил команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверил список портов командой (рис. 3.23)

Убедился, что порт 81 появился в списке.

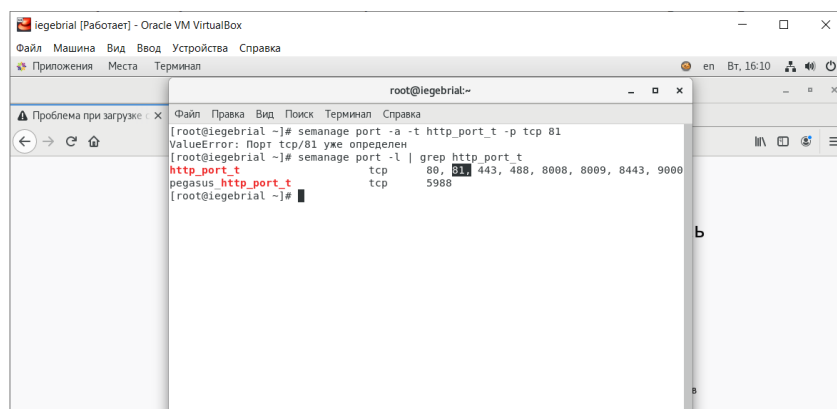


Figure 3.23: Добавление порта 81 и проверка список портов

20. Попробовал запустить веб-сервер Apache ещё раз. (рис. 3.24)

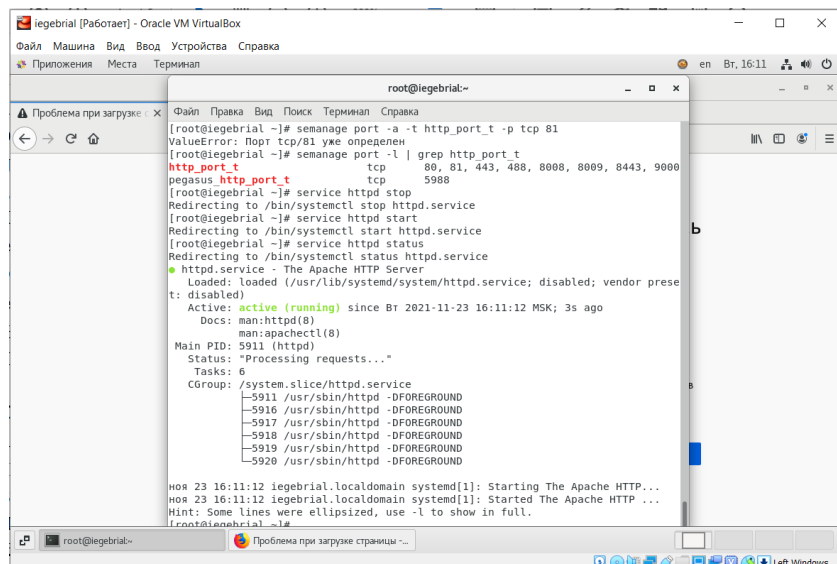


Figure 3.24: Попытка запуска веб-сервер Apache

21. Вернул контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`: (рис. 3.25)

`chcon -t httpd_sys_content_t /var/www/html/test.html`.



Figure 3.25: Возвращение контекста файла

22. Попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. (рис. 3.26)

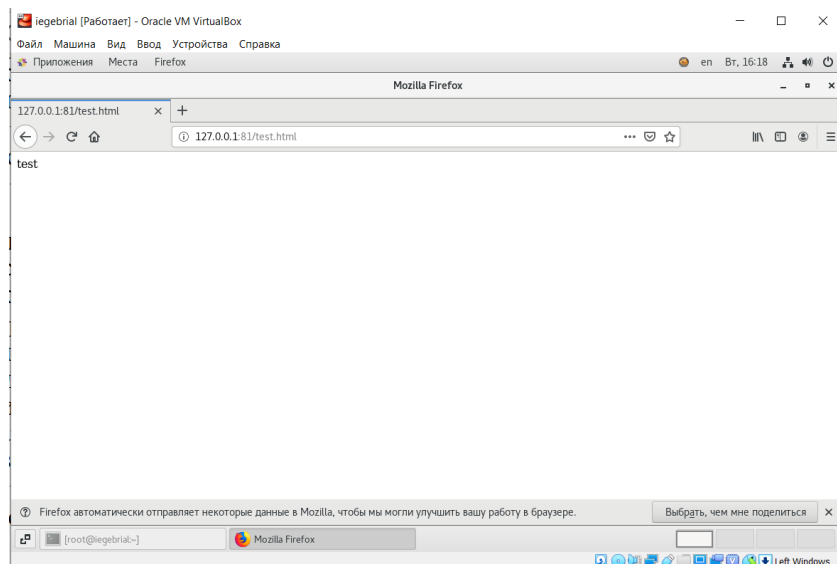


Figure 3.26: Попытка получения доступа к файлу через веб-сервер

23. Исправил обратно конфигурационный файл apache, вернув Listen 80. (рис. 3.27)

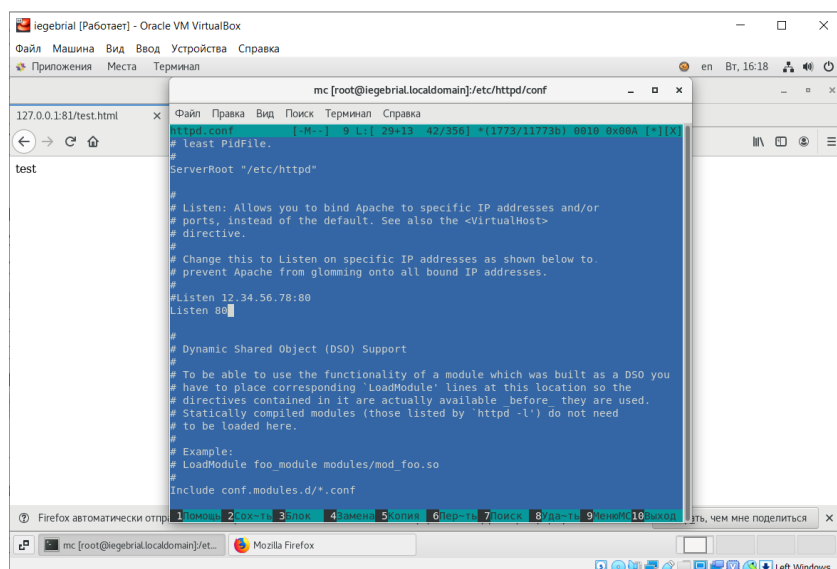
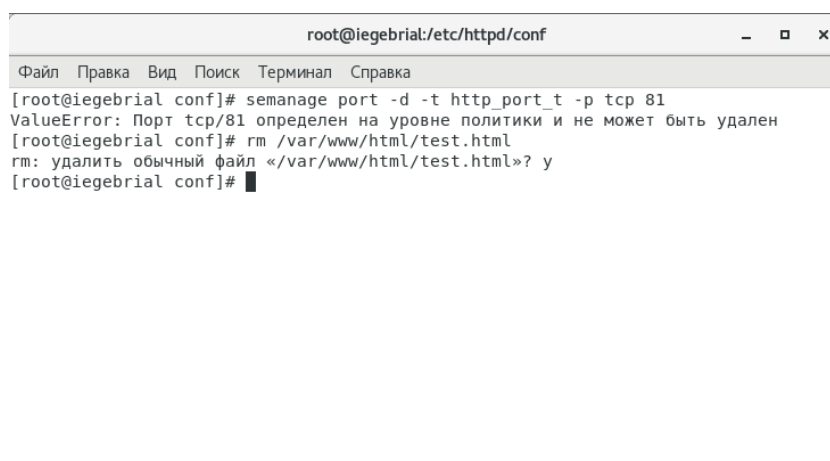


Figure 3.27: Исправления обратно конфигурационный файл apache

24. Удалил привязку http_port_t к 81 порту и удалил файл /var/www/html/test.html. (рис. 3.28)

Не получилось удалить привязку так как он определен на уровне политики.



```
root@iegebrial:/etc/httpd/conf
Файл  Правка  Вид  Поиск  Терминал  Справка
[root@iegebrial conf]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@iegebrial conf]# rm /var/www/html/test.html
rm: удалить обычный файл «/var/www/html/test.html»? y
[root@iegebrial conf]#
```

Figure 3.28: Удаление привязки http_port_t к 81 порту и файла /var/www/html/test.html

4 Выводы

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

5 Список литературы

1. Security-Enhanced Linux. Linux с улучшенной безопасностью: руководство пользователя / М. McAllister, S. Radvan, D. Walsh, D. Grift, E. Paris, J. Morris.
— URL: https://docs-old.fedoraproject.org/ru-RU/Fedora/13/html/Security-Enhanced_Linux/index.html.
2. SELinux – описание и особенности работы с системой. Часть 1: автор / itNews.
— URL: <https://habr.com/ru/company/kingservers/blog/209644/>. (дата обращения 20.01.2014).