

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.	11
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.	12
4.9	рис.9. Браузер и веб-сервер.	13
4.10	рис.10. Лог файлы.	14
4.11	рис.11. Лог файлы(часть 2).	15
4.12	рис.12. Запрет доступа к веб-серверу.	16
4.13	рис.13. Анализ ситуации.	17
4.14	рис.14. Лог веб-сервера.	18
4.15	рис.15. Listen 81.	19
4.16	рис.16. Неудачная попытка соединения с веб-сервером через браузер.	20
4.17	рис.17. Перезапуск сервера.	21
4.18	рис.18. Лог.	22
4.19	рис.19. Лог(часть2).	23
4.20	рис.20. Список портов.	24
4.21	рис.21. Повторный перезапуск сервера.	25
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

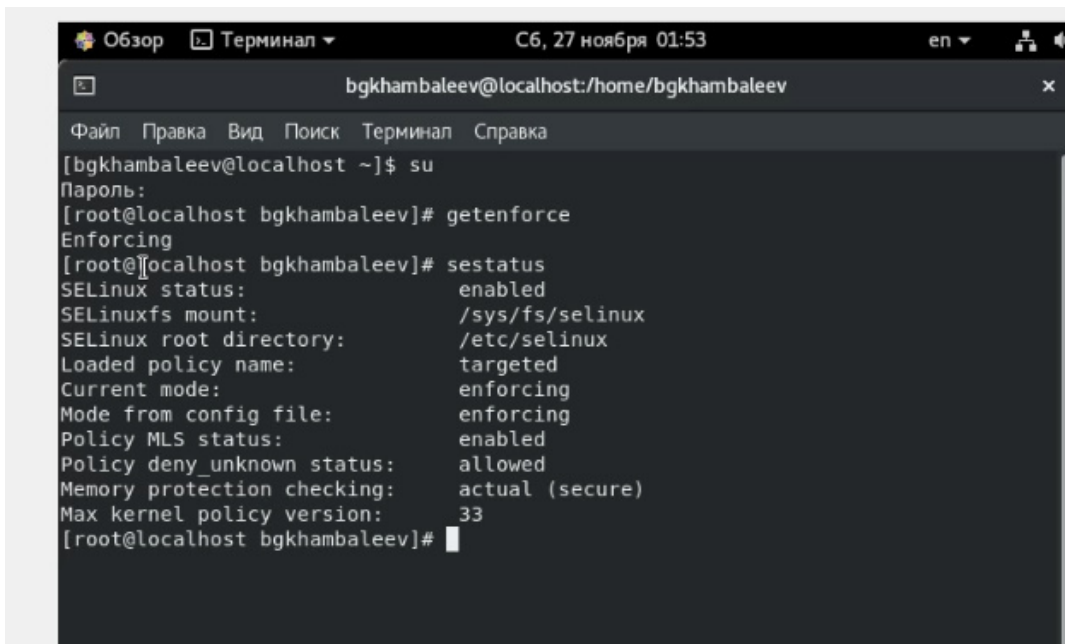
Лабораторная работа подразумевает использование некоторых консольных команд для взаимодействия с кодом и веб-сервером.

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)

A screenshot of a terminal window. The title bar shows 'Обзор Терминал' and the date/time 'Сб, 27 ноября 01:53'. The terminal content shows a user switching to root with 'su', then running 'getenforce' which returns 'Enforcing', and finally 'sestatus' which displays various SELinux configuration details.

```
bgkhambaleev@localhost: /home/bgkhambaleev
Файл Правка Вид Поиск Терминал Справка
[bgkhambaleev@localhost ~]$ su
Пароль:
[root@localhost bgkhambaleev]# getenforce
Enforcing
[root@localhost bgkhambaleev]# 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 bgkhambaleev]#
```

Figure 4.1: рис.1. Getenforce и sestatus.


```

httpd_can_network_connect      off
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_sss                 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
httpd_tmp_exec                 off
httpd_tty_comm                 off
httpd_unified                  off

```

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)

```

Netifcon:          0      Nodecon:          0

[root@localhost bgkhambaleev]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:      31 (MLS enabled)
Target Policy:        selinux
Handle unknown classes: allow
Classes:             132   Permissions:         463
Sensitivities:        1    Categories:         1024
Types:               4959  Attributes:          255
Users:               8     Roles:              14
Booleans:            340   Cond. Expr.:        389
Allow:              112894 Neverallow:          0
Auditallow:         166   Dontaudit:          10362
Type_trans:         253622 Type_change:          87
Type_member:         35   Range_trans:        6015
Role allow:         38    Role_trans:         423
Constraints:         72   Validatetrans:       0
MLS Constrains:     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 bgkhambaleev]#

```

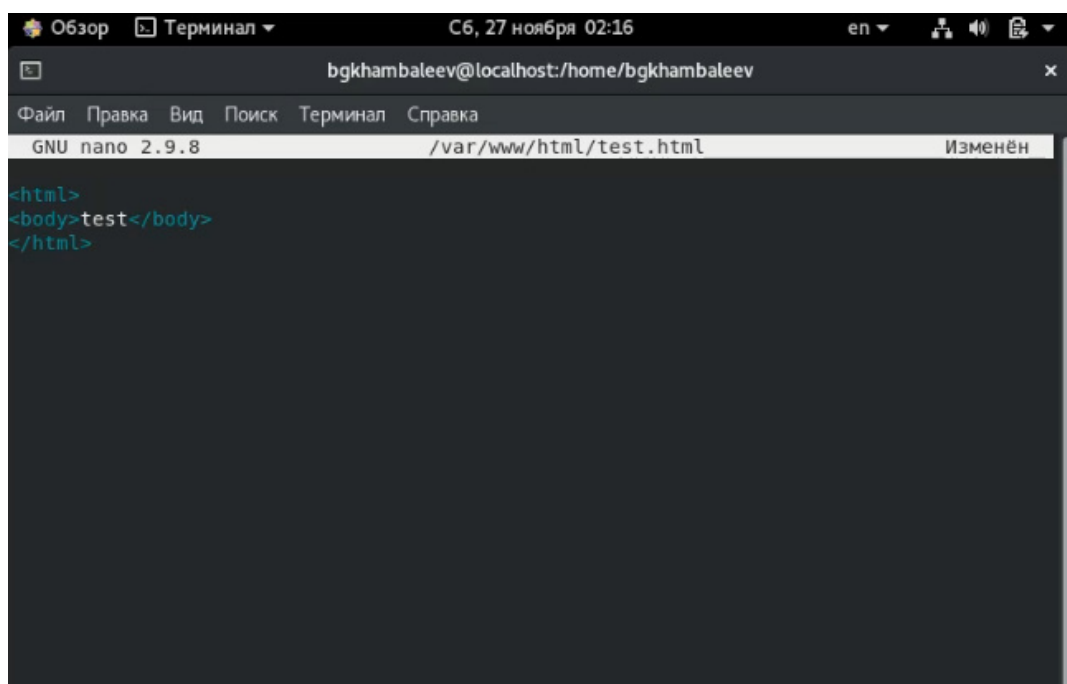
Figure 4.5: рис.5. Seinfo.

```

[root@localhost bgkhambaleev]# ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07:58 cgi
-bins
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 12 07:58 html
[root@localhost bgkhambaleev]# ls -lZ /var/www/html
итого 0
[root@localhost bgkhambaleev]# /var/www/html
bash: /var/www/html: Это каталог
[root@localhost bgkhambaleev]# su
[root@localhost bgkhambaleev]# exit
exit
[root@localhost bgkhambaleev]# exit
exit
[bgkhambaleev@localhost ~]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[bgkhambaleev@localhost ~]$ su
Пароль:
[root@localhost bgkhambaleev]# echo "test" > /var/www/html/test.txt
[root@localhost bgkhambaleev]# su guest
[guest@localhost bgkhambaleev]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[guest@localhost bgkhambaleev]$ su guest2
Пароль:
[guest2@localhost bgkhambaleev]$ echo "test" > /var/www/html/test1.txt
bash: /var/www/html/test1.txt: Отказано в доступе
[guest2@localhost bgkhambaleev]$

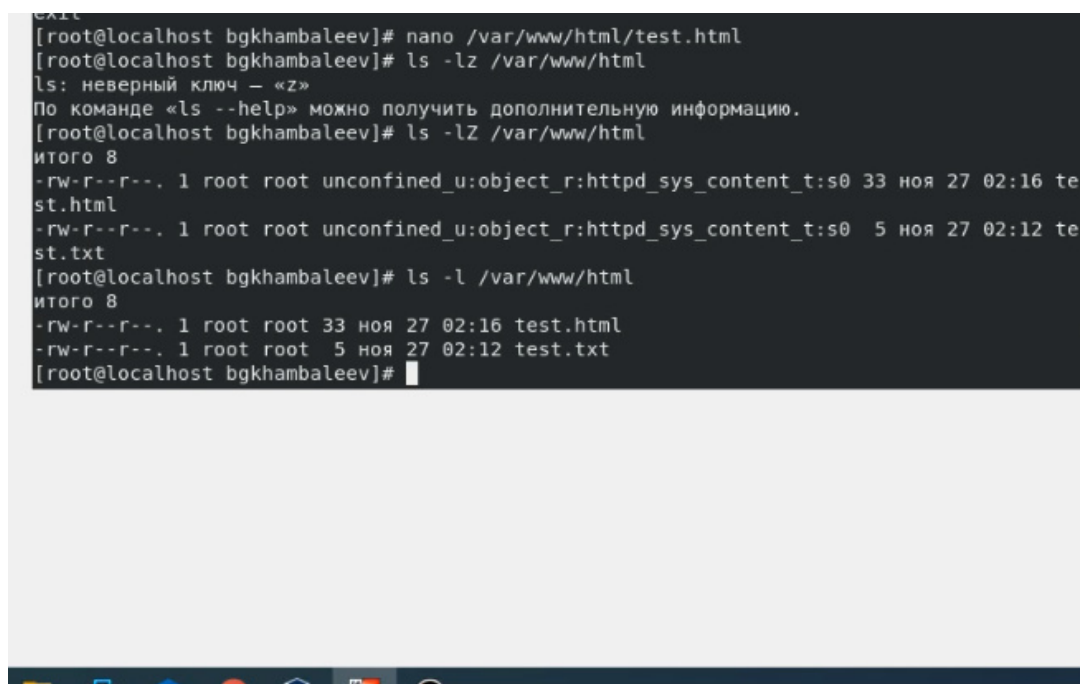
```

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



```
Обзор Терминал C6, 27 ноября 02:16 en
bgkhambaleev@localhost:/home/bgkhambaleev
Файл Правка Вид Поиск Терминал Справка
GNU nano 2.9.8 /var/www/html/test.html Изменён
<html>
<body>test</body>
</html>
```

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



```
EXIT
[root@localhost bgkhambaleev]# nano /var/www/html/test.html
[root@localhost bgkhambaleev]# ls -lz /var/www/html
ls: неверный ключ - «z»
По команде «ls --help» можно получить дополнительную информацию.
[root@localhost bgkhambaleev]# ls -lZ /var/www/html
итого 8
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 ноя 27 02:16 test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0  5 ноя 27 02:12 test.txt
[root@localhost bgkhambaleev]# ls -l /var/www/html
итого 8
-rw-r--r--. 1 root root 33 ноя 27 02:16 test.html
-rw-r--r--. 1 root root  5 ноя 27 02:12 test.txt
[root@localhost bgkhambaleev]#
```

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)

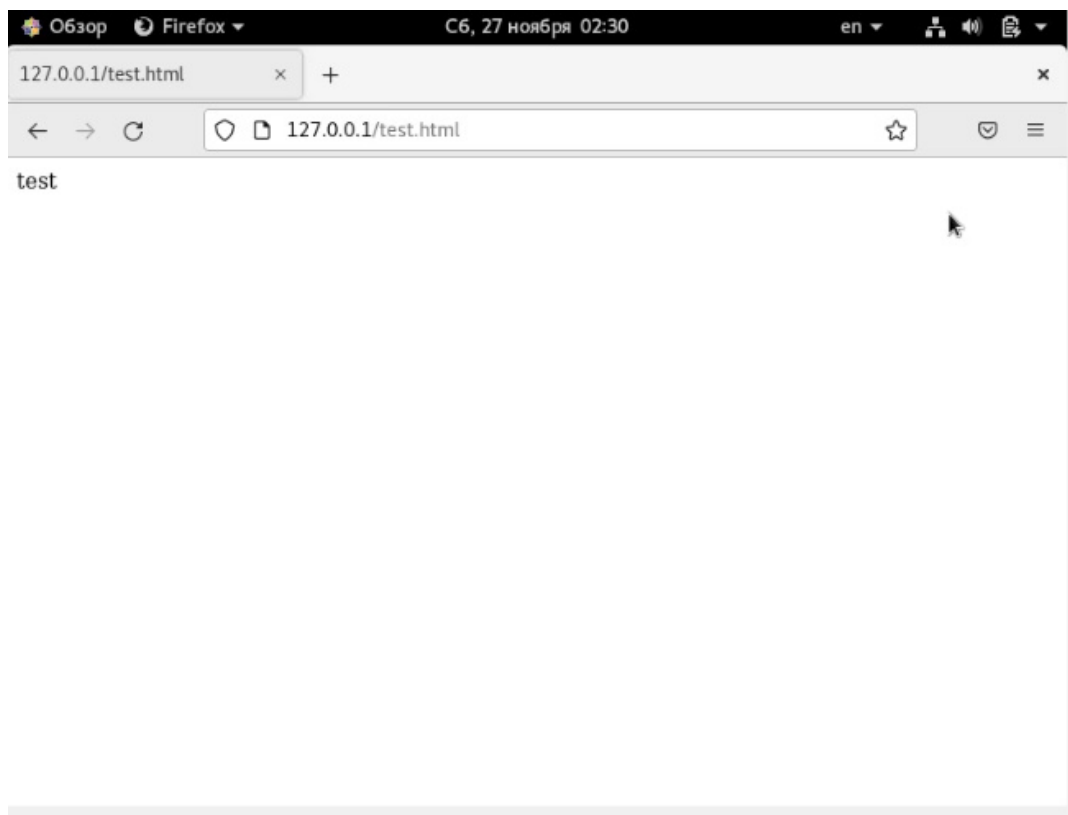
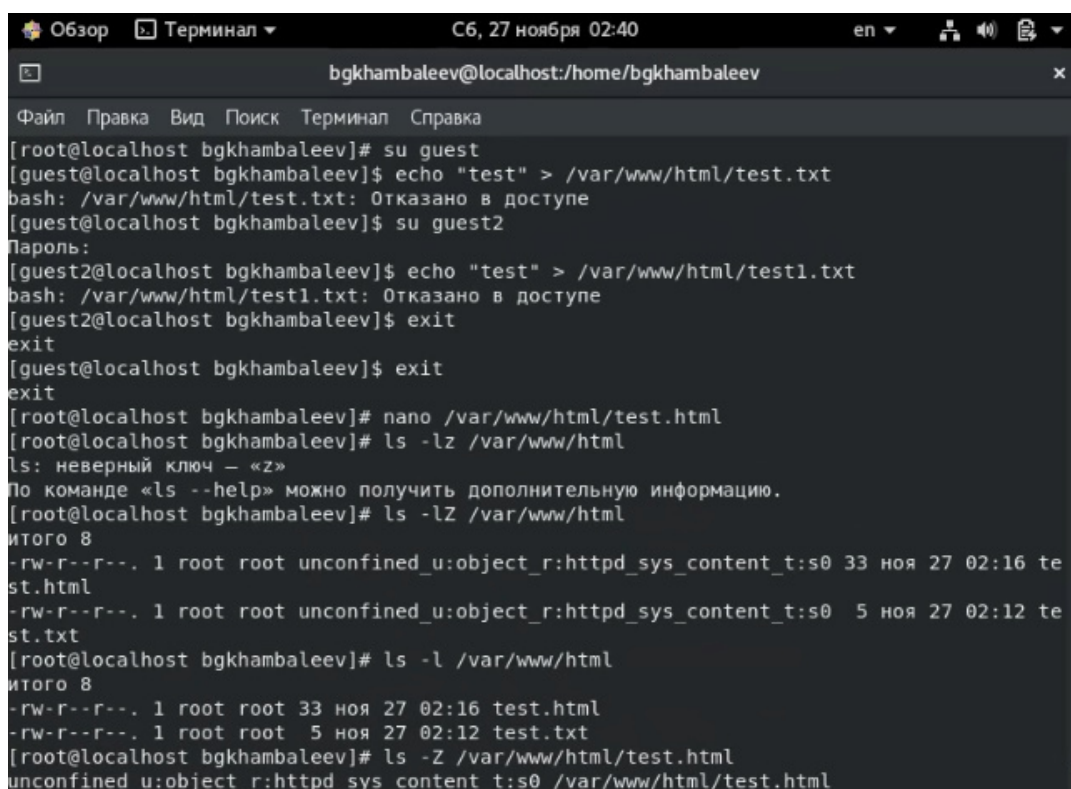


Figure 4.9: рис.9. Браузер и веб-сервер.



```
Обзор Терминал C6, 27 ноября 02:40 en
bgkhambaleev@localhost:/home/bgkhambaleev

Файл Правка Вид Поиск Терминал Справка
[root@localhost bgkhambaleev]# su guest
[guest@localhost bgkhambaleev]$ echo "test" > /var/www/html/test.txt
bash: /var/www/html/test.txt: Отказано в доступе
[guest@localhost bgkhambaleev]$ su guest2
Пароль:
[guest2@localhost bgkhambaleev]$ echo "test" > /var/www/html/test1.txt
bash: /var/www/html/test1.txt: Отказано в доступе
[guest2@localhost bgkhambaleev]$ exit
exit
[guest@localhost bgkhambaleev]$ exit
exit
[root@localhost bgkhambaleev]# nano /var/www/html/test.html
[root@localhost bgkhambaleev]# ls -lZ /var/www/html
ls: неверный ключ - «Z»
По команде «ls --help» можно получить дополнительную информацию.
[root@localhost bgkhambaleev]# ls -lZ /var/www/html
итого 8
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 ноя 27 02:16 te
st.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0  5 ноя 27 02:12 te
st.txt
[root@localhost bgkhambaleev]# ls -l /var/www/html
итого 8
-rw-r--r--. 1 root root 33 ноя 27 02:16 test.html
-rw-r--r--. 1 root root  5 ноя 27 02:12 test.txt
[root@localhost bgkhambaleev]# ls -Z /var/www/html/test.html
unconfined u:object r:httpd sys content t:s0 /var/www/html/test.html
```

Figure 4.10: рис.10. Лог файлы.

```
Обзор Терминал C6, 27 ноября 02:42 en
bgkhambaleev@localhost:/home/bgkhambaleev

Файл Правка Вид Поиск Терминал Справка
[guest@localhost bgkhambaleev]$ su guest2
Пароль:
[guest2@localhost bgkhambaleev]$ echo "test" > /var/www/html/test1.txt
bash: /var/www/html/test1.txt: Отказано в доступе
[guest2@localhost bgkhambaleev]$ exit
exit
[guest@localhost bgkhambaleev]$ exit
exit
[root@localhost bgkhambaleev]# nano /var/www/html/test.html
[root@localhost bgkhambaleev]# ls -lz /var/www/html
ls: неверный ключ - «z»
По команде «ls --help» можно получить дополнительную информацию.
[root@localhost bgkhambaleev]# ls -lZ /var/www/html
итого 8
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 ноя 27 02:16 test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0  5 ноя 27 02:12 test.txt
[root@localhost bgkhambaleev]# ls -l /var/www/html
итого 8
-rw-r--r--. 1 root root 33 ноя 27 02:16 test.html
-rw-r--r--. 1 root root  5 ноя 27 02:12 test.txt
[root@localhost bgkhambaleev]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@localhost bgkhambaleev]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost bgkhambaleev]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

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

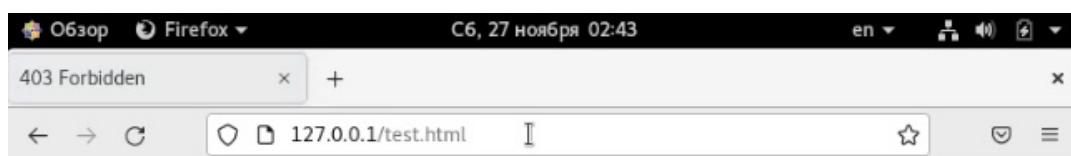
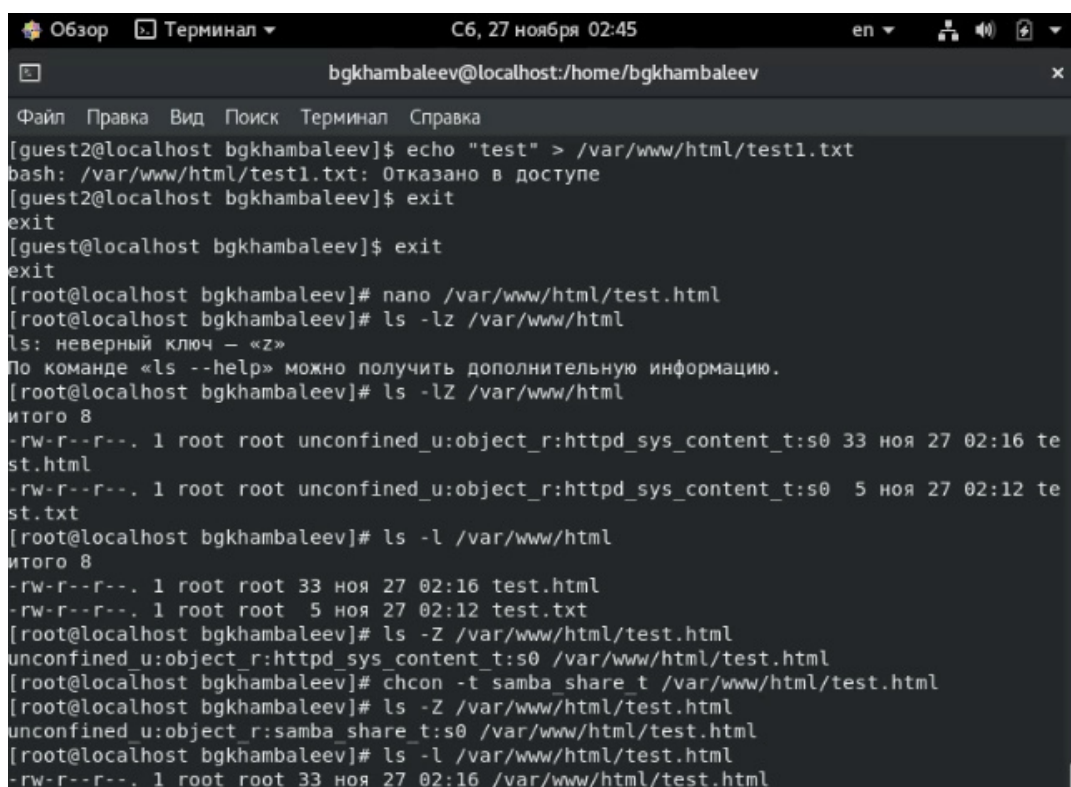


Figure 4.12: рис.12. Запрет доступа к веб-серверу.



```
Обзор Терминал C6, 27 ноября 02:45 en
bgkhambaleev@localhost:/home/bgkhambaleev

Файл Правка Вид Поиск Терминал Справка
[guest2@localhost bgkhambaleev]$ echo "test" > /var/www/html/test1.txt
bash: /var/www/html/test1.txt: Отказано в доступе
[guest2@localhost bgkhambaleev]$ exit
exit
[guest@localhost bgkhambaleev]$ exit
exit
[root@localhost bgkhambaleev]# nano /var/www/html/test.html
[root@localhost bgkhambaleev]# ls -lz /var/www/html
ls: неверный ключ - «z»
По команде «ls --help» можно получить дополнительную информацию.
[root@localhost bgkhambaleev]# ls -lZ /var/www/html
итого 8
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 ноя 27 02:16 te
st.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0  5 ноя 27 02:12 te
st.txt
[root@localhost bgkhambaleev]# ls -l /var/www/html
итого 8
-rw-r--r--. 1 root root 33 ноя 27 02:16 test.html
-rw-r--r--. 1 root root  5 ноя 27 02:12 test.txt
[root@localhost bgkhambaleev]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@localhost bgkhambaleev]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost bgkhambaleev]# ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@localhost bgkhambaleev]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 ноя 27 02:16 /var/www/html/test.html
```

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)

```
Обзор Терминал C6, 27 ноября 02:45 en
bgkhambaleev@localhost:/home/bgkhambaleev

Файл Правка Вид Поиск Терминал Справка
content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#01
2**** Plugin catchall (1.41 confidence) suggests *****#012#012
If you believe that httpd should be allowed getattr access on the test.html file by def
ault.#012Then you should report this as a bug.#012You can generate a local policy modul
e 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
Nov 27 02:44:08 localhost setroubleshoot[14694]: failed to retrieve rpm info for /var/w
ww/html/test.html
Nov 27 02:44:08 localhost setroubleshoot[14694]: SELinux is preventing /usr/sbin/httpd
from getattr access on the file /var/www/html/test.html. For complete SELinux messages
run: sealert -l 934506dd-d502-40f4-9967-7203656c3613
Nov 27 02:44:08 localhost setroubleshoot[14694]: SELinux is preventing /usr/sbin/httpd
from getattr access on the file /var/www/html/test.html.#012#012**** Plugin restoreco
n (92.2 confidence) suggests *****#012#012If you want to fix the l
abel. #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 pe
rmissions to access a parent directory in which case try to change the following comman
d accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/test.html#012#012**** Plu
gin 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#01
2**** Plugin catchall (1.41 confidence) suggests *****#012#012
If you believe that httpd should be allowed getattr access on the test.html file by def
ault.#012Then you should report this as a bug.#012You can generate a local policy modul
e 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 bgkhambaleev]#
```

Figure 4.14: рис.14. Лог веб-сервера.

```
bgkhambaleev@localhost:/home/bgkhambaleev
GNU nano 2.9.8 /etc/httpd/conf/httpd.conf

# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path.  If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used.  If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"
#
# 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
#

[ Wrote 356 lines ]
^G Помощь  ^O Записать  ^W Поиск    ^K Вырезать  ^J Выводить  ^C ТекПозиц
^X Выход    ^R ЧитФайл  ^\ Замена  ^U Отмен. выр ^T Словарь  ^_ К строке
```

Figure 4.15: рис.15. Listen 81.

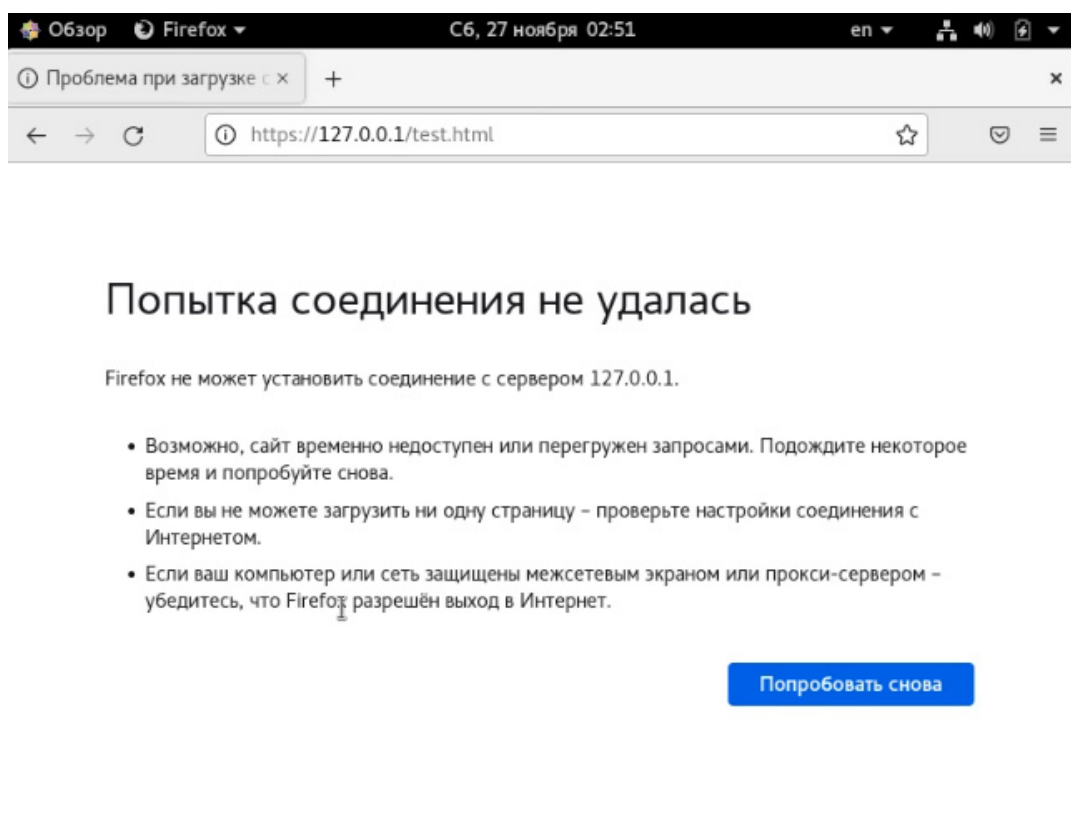
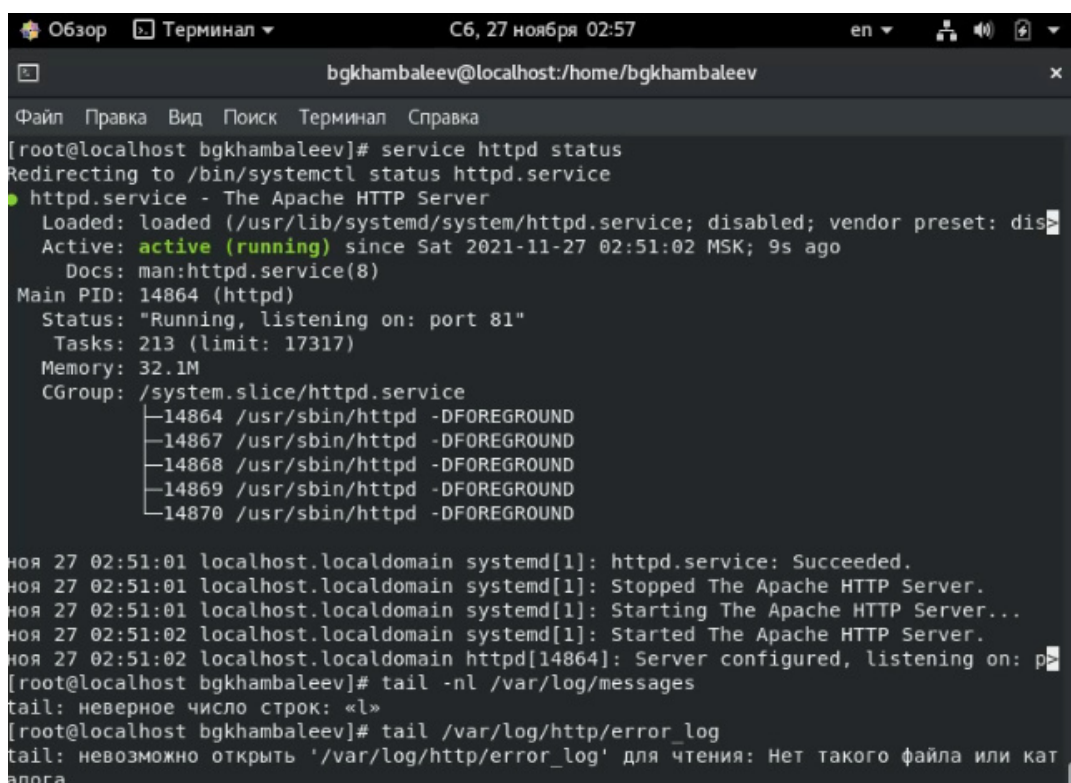


Figure 4.16: рис.16. Неудачная попытка соединения с веб-сервером через браузер.



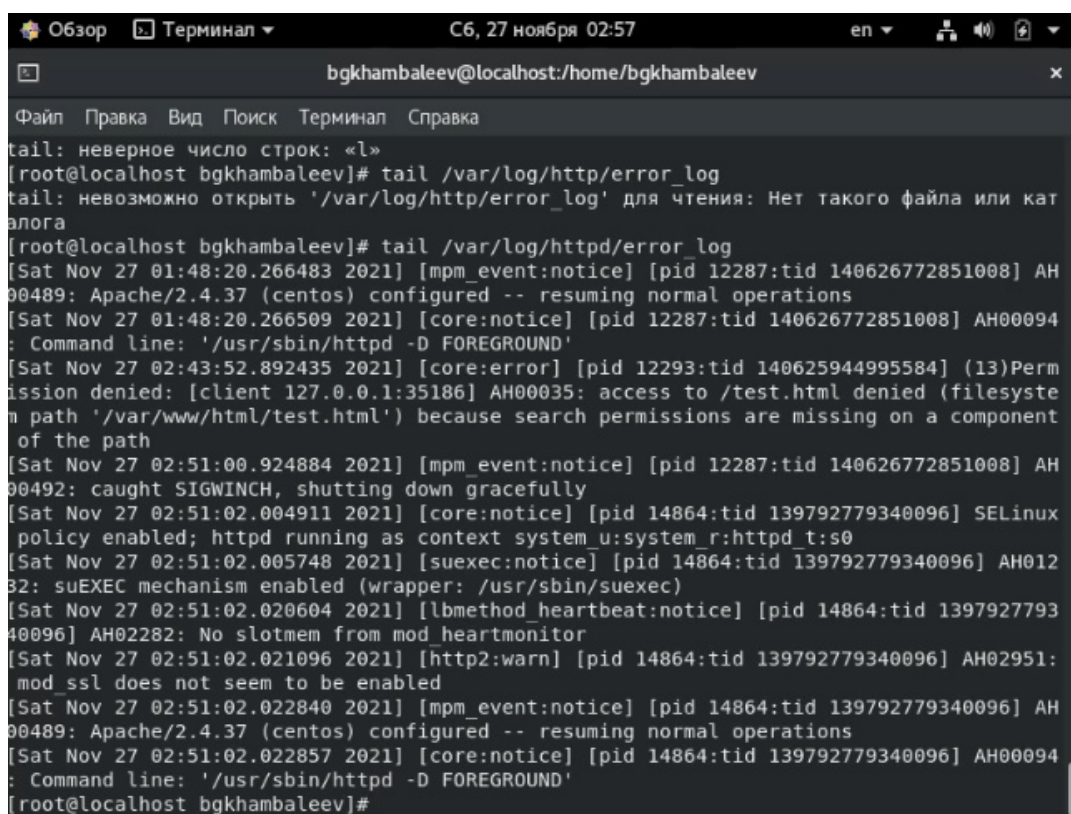
```
Обзор Терминал C6, 27 ноября 02:57 en
bgkhambaleev@localhost:/home/bgkhambaleev

Файл Правка Вид Поиск Терминал Справка
[root@localhost bgkhambaleev]# 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 preset: disabled)
   Active: active (running) since Sat 2021-11-27 02:51:02 MSK; 9s ago
     Docs: man:httpd.service(8)
  Main PID: 14864 (httpd)
    Status: "Running, listening on: port 81"
   Tasks: 213 (limit: 17317)
  Memory: 32.1M
    CGroup: /system.slice/httpd.service
            └─14864 /usr/sbin/httpd -DFOREGROUND
              └─14867 /usr/sbin/httpd -DFOREGROUND
                └─14868 /usr/sbin/httpd -DFOREGROUND
                  └─14869 /usr/sbin/httpd -DFOREGROUND
                    └─14870 /usr/sbin/httpd -DFOREGROUND

ноя 27 02:51:01 localhost.localdomain systemd[1]: httpd.service: Succeeded.
ноя 27 02:51:01 localhost.localdomain systemd[1]: Stopped The Apache HTTP Server.
ноя 27 02:51:01 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 27 02:51:02 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
ноя 27 02:51:02 localhost.localdomain httpd[14864]: Server configured, listening on: p
[root@localhost bgkhambaleev]# tail -nl /var/log/messages
tail: неверное число строк: «l»
[root@localhost bgkhambaleev]# tail /var/log/http/error_log
tail: невозможно открыть '/var/log/http/error_log' для чтения: Нет такого файла или каталога
```

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)



The image shows a terminal window titled "Обзор Терминал" with a subtitle "C6, 27 ноября 02:57". The user is logged in as "bgkhambaleev" at "localhost". The terminal shows the following commands and output:

```
tail: неверное число строк: «1»
[root@localhost bgkhambaleev]# tail /var/log/http/error_log
tail: невозможно открыть '/var/log/http/error_log' для чтения: Нет такого файла или каталога
[root@localhost bgkhambaleev]# tail /var/log/httpd/error_log
[Sat Nov 27 01:48:20.266483 2021] [mpm_event:notice] [pid 12287:tid 140626772851008] AH00489: Apache/2.4.37 (centos) configured -- resuming normal operations
[Sat Nov 27 01:48:20.266509 2021] [core:notice] [pid 12287:tid 140626772851008] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Sat Nov 27 02:43:52.892435 2021] [core:error] [pid 12293:tid 140625944995584] (13)Permission denied: [client 127.0.0.1:35186] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Sat Nov 27 02:51:00.924884 2021] [mpm_event:notice] [pid 12287:tid 140626772851008] AH00492: caught SIGWINCH, shutting down gracefully
[Sat Nov 27 02:51:02.004911 2021] [core:notice] [pid 14864:tid 139792779340096] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Nov 27 02:51:02.005748 2021] [suexec:notice] [pid 14864:tid 139792779340096] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sat Nov 27 02:51:02.020604 2021] [lbmethod_heartbeat:notice] [pid 14864:tid 139792779340096] AH02282: No slotmem from mod_heartbeat
[Sat Nov 27 02:51:02.021096 2021] [http2:warn] [pid 14864:tid 139792779340096] AH02951: mod_ssl does not seem to be enabled
[Sat Nov 27 02:51:02.022840 2021] [mpm_event:notice] [pid 14864:tid 139792779340096] AH00489: Apache/2.4.37 (centos) configured -- resuming normal operations
[Sat Nov 27 02:51:02.022857 2021] [core:notice] [pid 14864:tid 139792779340096] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[root@localhost bgkhambaleev]#
```

Figure 4.18: рис.18. Лог.


```
Обзор Терминал C6, 27 ноября 02:58 en
bgkhambaleev@localhost:/home/bgkhambaleev

Файл Правка Вид Поиск Терминал Справка
bd 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(1637970232.890:310): proctitle=2F7573722F7362696E2F68747470640
02D44464F524547524F554E44
type=AVC msg=audit(1637970232.890:311): avc: denied { getattr } for pid=12293 comm="
httpd" path="/var/www/html/test.html" dev="dm-0" ino=1266723 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(1637970232.890:311): arch=c000003e syscall=6 success=no exit=-13
a0=7fe60c045d30 a1=7fe6077f5890 a2=7fe6077f5890 a3=1 items=0 ppid=12287 pid=12293 auid
=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=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=lststat AUID="unset" UID="apache" GID="apache" EUID="apache"
SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1637970232.890:311): proctitle=2F7573722F7362696E2F68747470640
02D44464F524547524F554E44
type=SERVICE_STOP msg=audit(1637970661.949:312): pid=1 uid=0 auid=4294967295 ses=429496
7295 subj=system_u:system_r:init t:s0 msg='unit=httpd comm="systemd" exe="/usr/lib/syst
emd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="unset"
type=SERVICE_START msg=audit(1637970662.013:313): pid=1 uid=0 auid=4294967295 ses=42949
67295 subj=system_u:system_r:init t:s0 msg='unit=httpd comm="systemd" exe="/usr/lib/sys
temd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="unset"
type=SERVICE_START msg=audit(1637970821.861:314): pid=1 uid=0 auid=4294967295 ses=42949
67295 subj=system_u:system_r:init t:s0 msg='unit=dnf-makecache comm="systemd" exe="/usr
/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1637970821.861:315): pid=1 uid=0 auid=4294967295 ses=429496
7295 subj=system_u:system_r:init t:s0 msg='unit=dnf-makecache comm="systemd" exe="/usr/
lib/systemd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="unset"
[root@localhost bgkhambaleev]#
```

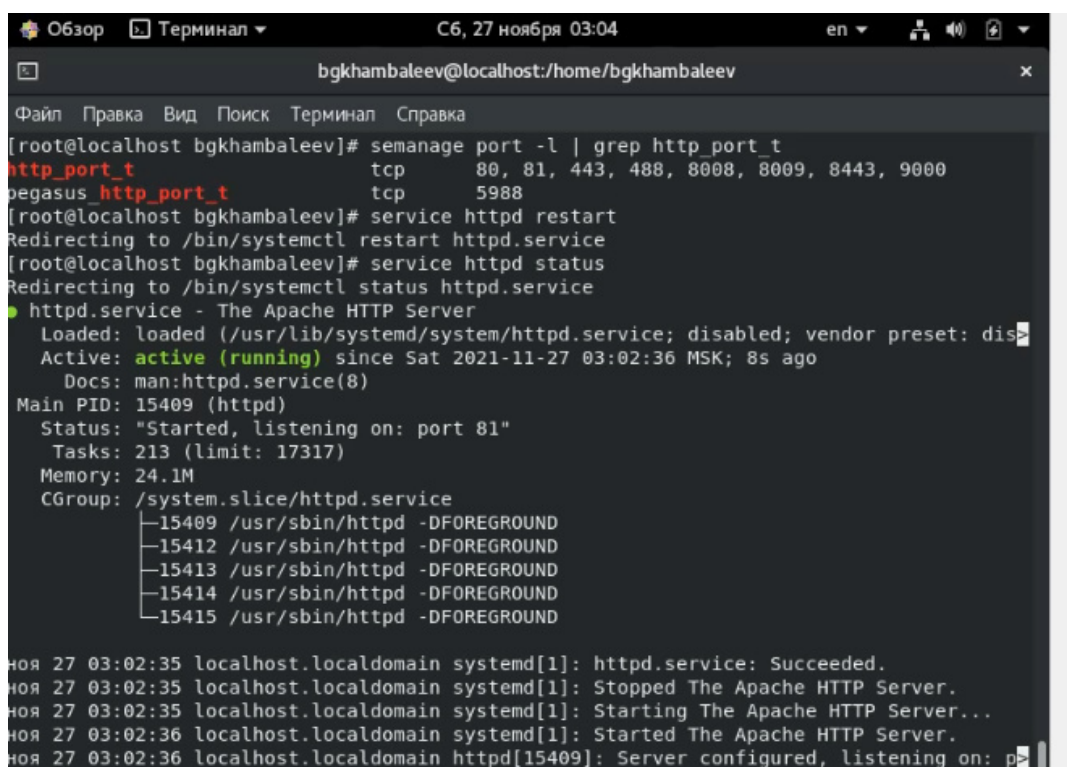
Figure 4.19: рис.19. Лог(часть2).

```
Обзор Терминал C6, 27 ноября 03:01 en
bgkhambaleev@localhost:/home/bgkhambaleev

Файл Правка Вид Поиск Терминал Справка

httpd" path="/var/www/html/test.html" dev="dm-0" ino=1266723 scontext=system_u:system_r
:htp d t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1637970232.890:311): arch=c000003e syscall=6 success=no exit=-13
a0=7fe60c045d30 a1=7fe6077f5890 a2=7fe6077f5890 a3=1 items=0 ppid=12287 pid=12293 auid
=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none)
ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:htp d t:s0 key
=(null) ARCH=x86_64 SYSCALL=lst at AUID="unset" UID="apache" GID="apache" EUID="apache"
SUID="apache" FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1637970232.890:311): proctitle=2F7573722F7362696E2F68747470640
02D44464F524547524F554E44
type=SERVICE_STOP msg=audit(1637970661.949:312): pid=1 uid=0 auid=4294967295 ses=429496
7295 subj=system_u:system_r:init_t:s0 msg='unit=httpd comm="systemd" exe="/usr/lib/syst
emd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="unset"
type=SERVICE_START msg=audit(1637970662.013:313): pid=1 uid=0 auid=4294967295 ses=42949
67295 subj=system_u:system_r:init_t:s0 msg='unit=httpd comm="systemd" exe="/usr/lib/sys
temd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="unset"
type=SERVICE_START msg=audit(1637970821.861:314): pid=1 uid=0 auid=4294967295 ses=42949
67295 subj=system_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="systemd" exe="/usr
/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="unset"
type=SERVICE_STOP msg=audit(1637970821.861:315): pid=1 uid=0 auid=4294967295 ses=429496
7295 subj=system_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="systemd" exe="/usr/
lib/systemd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="unset"
[root@localhost bgkhambaleev]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@localhost bgkhambaleev]# 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 bgkhambaleev]#
```

Figure 4.20: рис.20. Список портов.



```
Обзор Терминал C6, 27 ноября 03:04 en
bgkhambaleev@localhost:/home/bgkhambaleev

Файл Правка Вид Поиск Терминал Справка
[root@localhost bgkhambaleev]# 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 bgkhambaleev]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@localhost bgkhambaleev]# 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 preset: disabled)
   Active: active (running) since Sat 2021-11-27 03:02:36 MSK; 8s ago
     Docs: man:httpd.service(8)
   Main PID: 15409 (httpd)
   Status: "Started, listening on: port 81"
    Tasks: 213 (limit: 17317)
  Memory: 24.1M
   CGroup: /system.slice/httpd.service
           └─15409 /usr/sbin/httpd -DFOREGROUND
             └─15412 /usr/sbin/httpd -DFOREGROUND
               └─15413 /usr/sbin/httpd -DFOREGROUND
                 └─15414 /usr/sbin/httpd -DFOREGROUND
                   └─15415 /usr/sbin/httpd -DFOREGROUND

ноя 27 03:02:35 localhost.localdomain systemd[1]: httpd.service: Succeeded.
ноя 27 03:02:35 localhost.localdomain systemd[1]: Stopped The Apache HTTP Server.
ноя 27 03:02:35 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 27 03:02:36 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
ноя 27 03:02:36 localhost.localdomain httpd[15409]: Server configured, listening on: p
```

Figure 4.21: рис.21. Повторный перезапуск сервера.

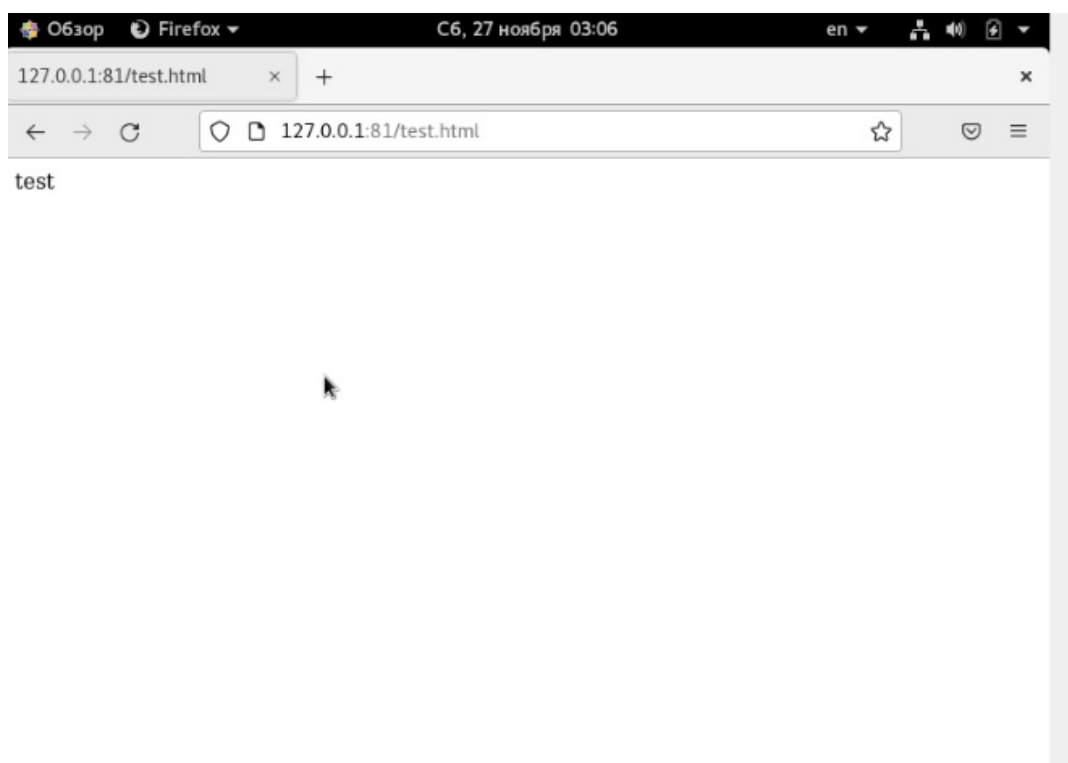
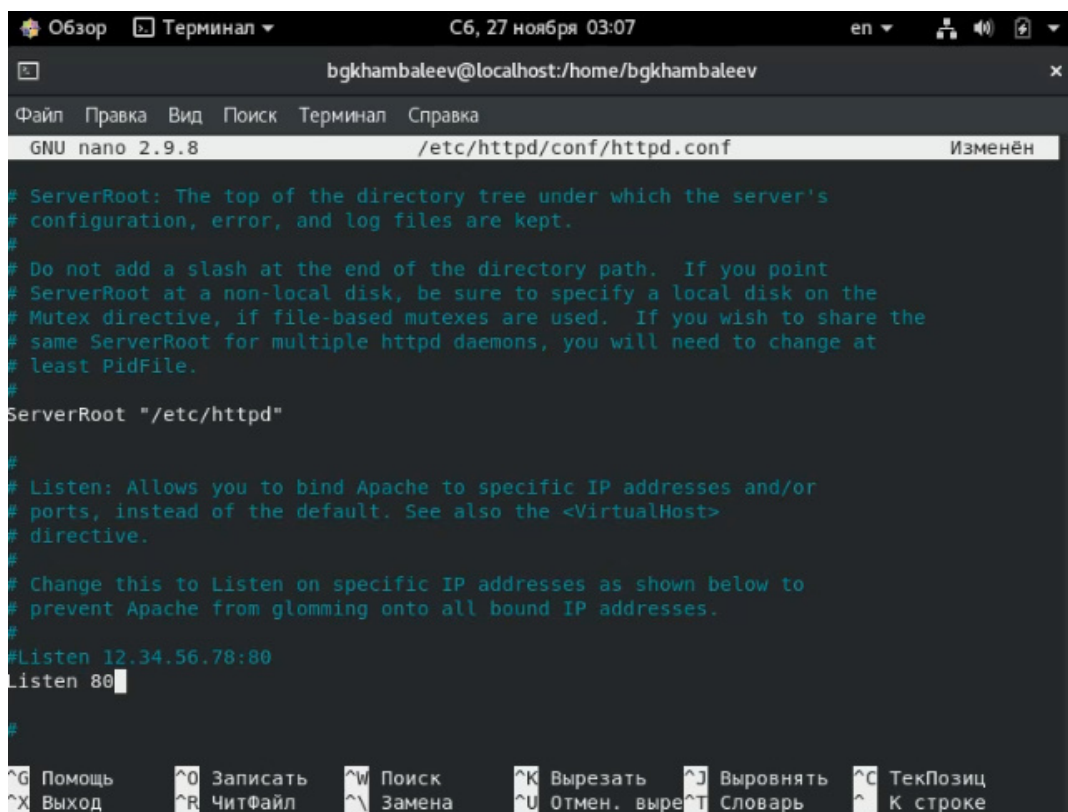


Figure 4.22: рис.22. Удачная попытка доступа к серверу.

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



```
bgkhambaleev@localhost: /home/bgkhambaleev
GNU nano 2.9.8 /etc/httpd/conf/httpd.conf Изменён

# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path.  If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used.  If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"
#
# 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 80
#

^G Помощь      ^O Записать    ^W Поиск      ^K Вырезать    ^J Выводить    ^C ТекПозиц
^X Выход      ^R ЧитФайл    ^\ Замена     ^U Отмен. выр  ^T Словарь     ^_ К строке
```

Figure 4.23: рис.23. Исправление конфигурационного файла.

```
Обзор Терминал C6, 27 ноября 03:11 en
bgkhambaleev@localhost:/home/bgkhambaleev

Файл Правка Вид Поиск Терминал Справка
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Sat 2021-11-27 03:02:36 MSK; 8s ago
     Docs: man:httpd.service(8)
   Main PID: 15409 (httpd)
   Status: "Started, listening on: port 81"
   Tasks: 213 (limit: 17317)
  Memory: 24.1M
   CGroup: /system.slice/httpd.service
           └─15409 /usr/sbin/httpd -DFOREGROUND
             └─15412 /usr/sbin/httpd -DFOREGROUND
               └─15413 /usr/sbin/httpd -DFOREGROUND
                 └─15414 /usr/sbin/httpd -DFOREGROUND
                   └─15415 /usr/sbin/httpd -DFOREGROUND

ноя 27 03:02:35 localhost.localdomain systemd[1]: httpd.service: Succeeded.
ноя 27 03:02:35 localhost.localdomain systemd[1]: Stopped The Apache HTTP Server.
ноя 27 03:02:35 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 27 03:02:36 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
ноя 27 03:02:36 localhost.localdomain httpd[15409]: Server configured, listening on: p
[root@localhost bgkhambaleev]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@localhost bgkhambaleev]# nano /etc/httpd/conf/httpd.conf
[root@localhost bgkhambaleev]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@localhost bgkhambaleev]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@localhost bgkhambaleev]#
```

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

5 Библиография

- [illegible]

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.