

Отчёт по лабораторной работе №6

дисциплина: Информационная безопасность

Фогилева ксения Михайловна

Содержание

1	Цель работы	5
2	Теоретическое описание	6
3	Выполнение лабораторной работы	7
4	Выводы	19

List of Tables

List of Figures

3.1	Проверка	7
3.2	Проверка	7
3.3	веб-сервер Apache	8
3.4	Просмотр состояние переключателей SELinux для Apache	8
3.5	Получение информации	9
3.6	Создание файла	10
3.7	Проверка	10
3.8	Получение доступа к файлу через браузер	11
3.9	Проверка контекста	11
3.10	Изменение контекста, проверка	11
3.11	Получение доступа к файлу через браузер	12
3.12	Проверка	12
3.13	Просмотр системного лог-файла	13
3.14	Изменеие порта 80 на 81	13
3.15	Анализ лог-файла	14
3.16	Просмотр файла /var/log/http/access_log	14
3.17	Просмотр файла /var/log/http/error_log	15
3.18	Просмотр файла var/log/audit/audit.log	15
3.19	Выполнение и проверка	16
3.20	Возвращение контекста	16
3.21	Получение доступа к файлу через браузер	17
3.22	Исправление конфигурационного файл apache	17
3.23	Удалние привязки http_port_t к 81 порту	18
3.24	Удаление файла /var/www/html/test.html	18

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 Теоретическое описание

SELinux — набор технологий расширения системы безопасности Linux. Сегодня основу набора составляют три технологии: мандатный контроль доступа, ролевой доступ RBAC и система типов (доменов). Apache – это свободное программное обеспечение для размещения веб-сервера. Он хорошо показывает себя в работе с масштабными проектами, поэтому заслуженно считается одним из самых популярных веб-серверов. Кроме того, Apache очень гибок в плане настройки, что даёт возможность реализовать все особенности размещаемого веб-ресурса.

3 Выполнение лабораторной работы

1. Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`. (рис. 3.1).

```
guest@kmfogleva ~]$ getenforce
Enforcing
guest@kmfogleva ~]$ 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
guest@kmfogleva ~]$
```

Figure 3.1: Проверка

2. Обратилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает: `service httpd status` (рис. 3.2).

```
guest@kmfogleva ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2021-11-25 13:56:37 MSK; 2h 56min ago
     Docs: man:httpd.service(8)
   Main PID: 33853 (httpd)
    Status: "Running, listening on: port 80"
     Tasks: 213 (limit: 4812)
    Memory: 24.3M
    CGroup: /system.slice/httpd.service
            └─33853 /usr/sbin/httpd -DFOREGROUND
              └─33860 /usr/sbin/httpd -DFOREGROUND
                └─33861 /usr/sbin/httpd -DFOREGROUND
                  └─33862 /usr/sbin/httpd -DFOREGROUND
                    └─33863 /usr/sbin/httpd -DFOREGROUND
lines 1-14/14 (END)
```

Figure 3.2: Проверка

3. Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности. (рис. 3.3).

```

system_u:system_r:httpd_t:s0  apache  33861  0.0  1.2  1354568  10376  ?  Sl  1
3:56  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  33862  0.0  1.4  1485696  12364  ?  Sl  1
3:56  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  33863  0.0  1.2  1354568  10380  ?  Sl  1
3:56  0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-c0.c1023 guest 34755 0.0 0.1 12136 1196 p
ts/0 $+ 16:54 0:00 grep --color=auto httpd
[guest@kmfogleva ~]$

```

Figure 3.3: веб-сервер Apache

- Посмотрела текущее состояние переключателей SELinux для Apache с помощью команды: `sestatus -bigrep httpd`. Обратила внимание, что многие из них находятся в положении «off». (рис. 3.4).

```

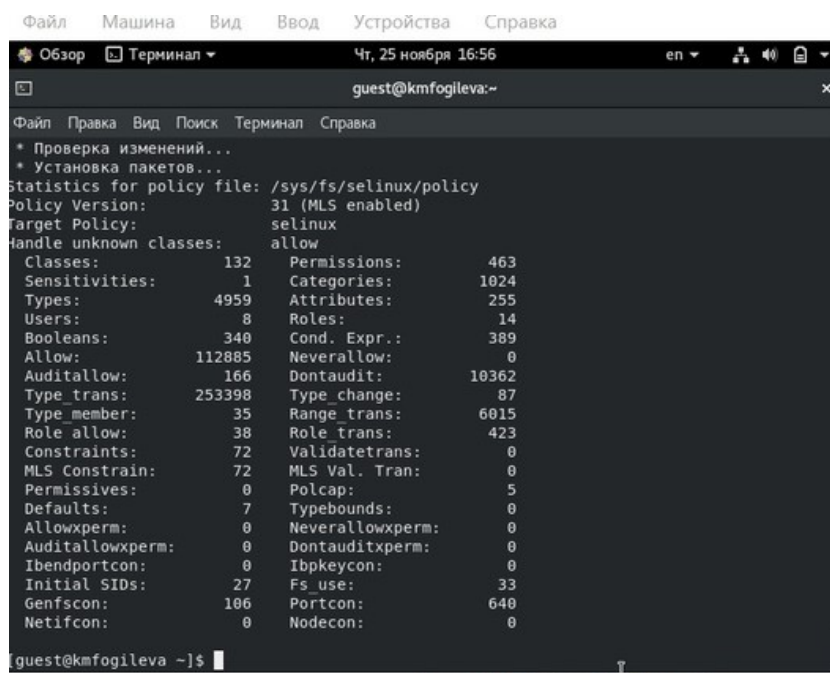
virt_use_samba                off
virt_use_sanlock              off
virt_use_usb                  on
virt_use_xserver              off
webadm_manage_user_files     off
webadm_read_user_files       off
wine_mmap_zero_ignore        off
xdm_bind_vnc_tcp_port        off
xdm_exec_bootloader          off
xdm_sysadm_login             off
xdm_write_home                off
xen_use_nfs                   off
xend_run_blktp               on
xend_run_qemu                on
xquest_connect_network       on
xquest_exec_content          on
xquest_mount_media           on
xquest_use_bluetooth         on
xserver_clients_write_xshm   off
xserver_execmem              off
xserver_object_manager       off
zabbix_can_network           off
zabbix_run_sudo              off
zarafe_setrlimit             off
zebra_write_config           off
zoneminder_anon_write        off
zoneminder_run_sudo          off
[guest@kmfogleva ~]$

```

Figure 3.4: Просмотр состояние переключателей SELinux для Apache

- Посмотрела статистику по политике с помощью команды `seinfo`, также определила множество пользователей(8), ролей(14), типов(4793). Определила тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды: `ls -lZ /var/www`. Определила тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`. Определила круг пользо-

вателей, которым разрешено создание файлов в директории /var/www/html.
(рис. 3.5).



The screenshot shows a terminal window titled "guest@kmfogileva:~" with a menu bar containing "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". The terminal output displays the command "seinfo -a" and its results, which are statistics for the SELinux policy file located at /sys/fs/selinux/policy. The output includes information about the policy version (31, MLS enabled), target policy (selinux), and a detailed breakdown of various SELinux classes and their associated permissions, categories, attributes, and other metrics.

```
Файл  Правка  Вид  Поиск  Терминал  Справка
* Проверка изменений...
* Установка пакетов...
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          31 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                  132
Sensitivities:            1
Types:                    4959
Users:                    8
Booleans:                 340
Allow:                    112885
Auditallow:               166
Type_trans:               253398
Type_member:              35
Role_allow:               38
Constraints:              72
MLS Constrain:            72
Permissives:              0
Defaults:                 7
Allowxperm:               0
Auditallowxperm:          0
Ibendportcon:             0
Initial SIDs:             27
Genfscon:                 106
Netifcon:                 0
Permissions:              463
Categories:              1024
Attributes:               255
Roles:                    14
Cond. Expr.:              389
Neverallow:               0
Dontaudit:                10362
Type_change:              87
Range_trans:              6015
Role_trans:               423
Validatetrans:            0
MLS Val. Tran:            0
Polcap:                   5
Typebounds:               0
Neverallowxperm:          0
Dontauditxperm:           0
Ibpkeycon:                0
Fs_use:                   33
Portcon:                  640
Nodecon:                  0
guest@kmfogileva ~]$
```

Figure 3.5: Получение информации

6. Создала от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл /var/www/html/test.html(рис. 3.6).

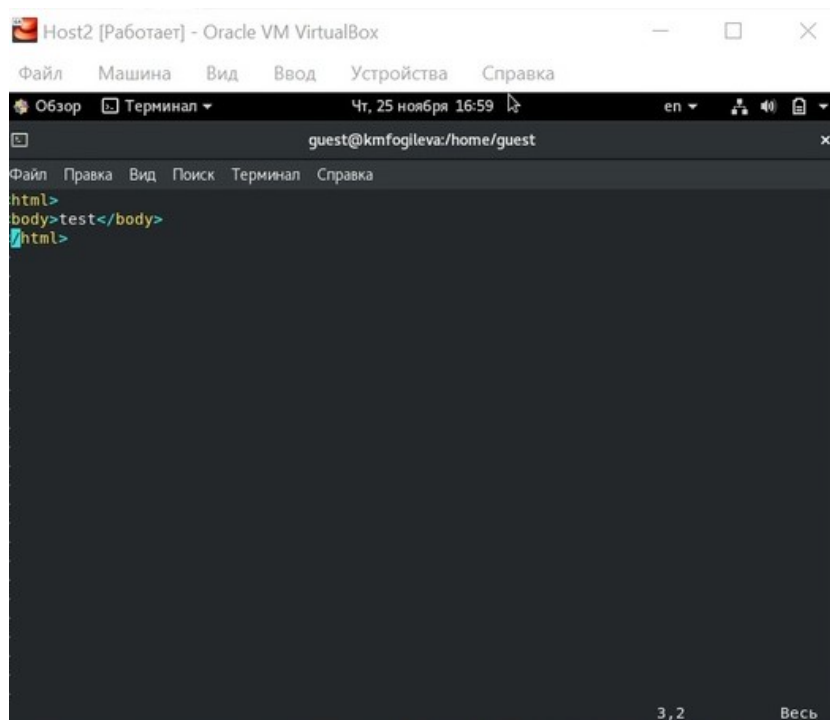


Figure 3.6: Создание файла

7. Проверила контекст созданного файла. httpd_sys_content_t (рис. 3.7).

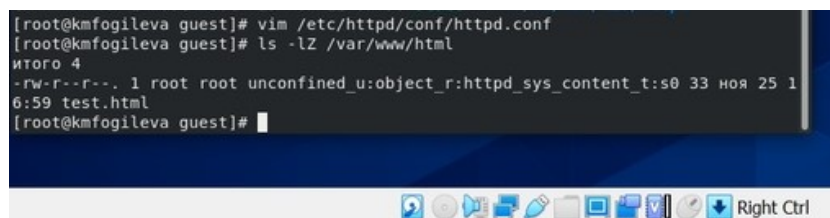


Figure 3.7: Проверка

8. Обратилась к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>. Убедилась, что файл был успешно отображён. (рис. 3.8).

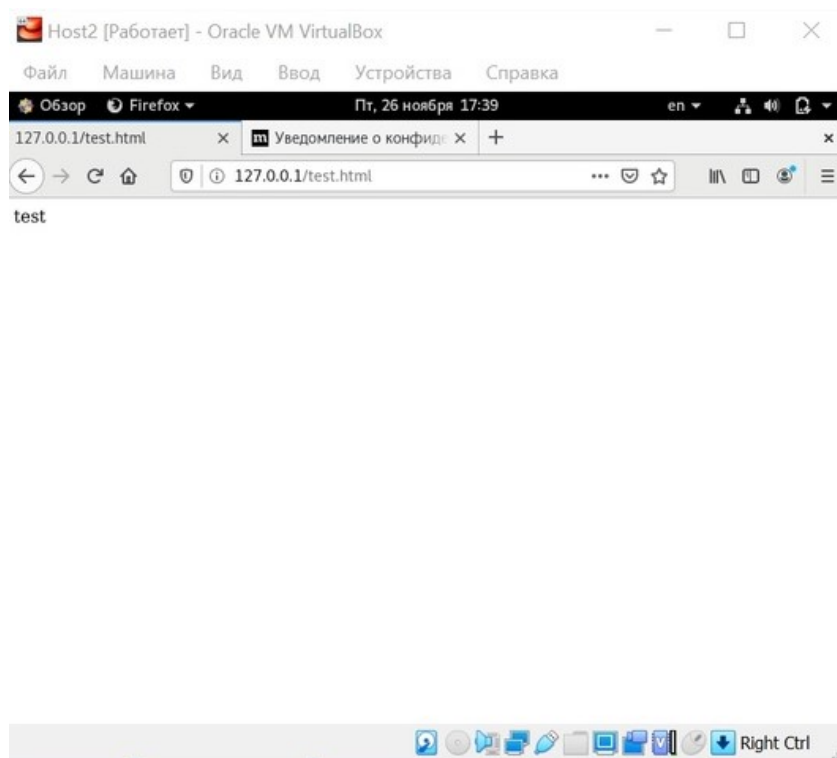


Figure 3.8: Получение доступа к файлу через браузер

9. Проверила контекст файла командой: `ls -Z /var/www/html/test.html` (рис. 3.9).

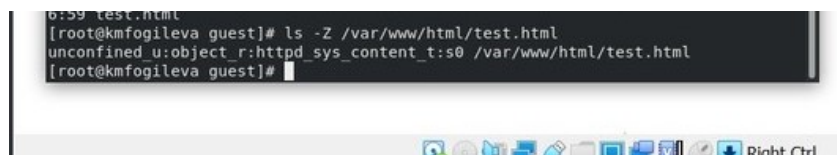


Figure 3.9: Проверка контекста

10. Изменила контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`. После этого проверила, что контекст поменялся. (рис. 3.10).



Figure 3.10: Изменение контекста, проверка

11. Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Получили сообщение об ошибке. (рис. 3.11).

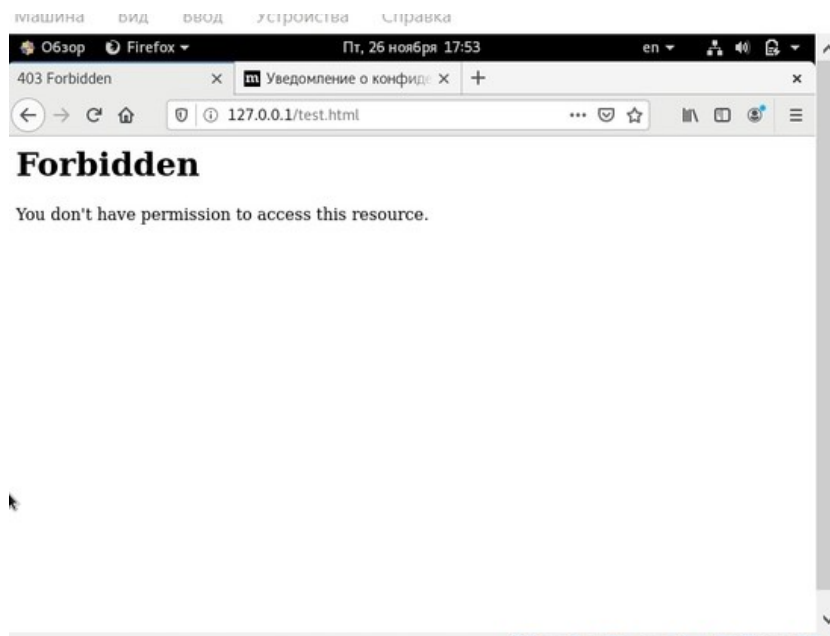


Figure 3.11: Получение доступа к файлу через браузер

12. Проанализировала ситуацию. Файл не был отображён потому что мы изменили контекст файла. Просмотрела log-файлы веб-сервера Apache. Также просмотрела системный лог-файл: `tail /var/log/messages` (рис. 3.12), (рис. 3.13).

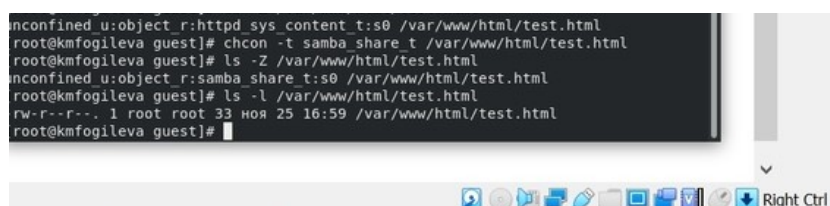
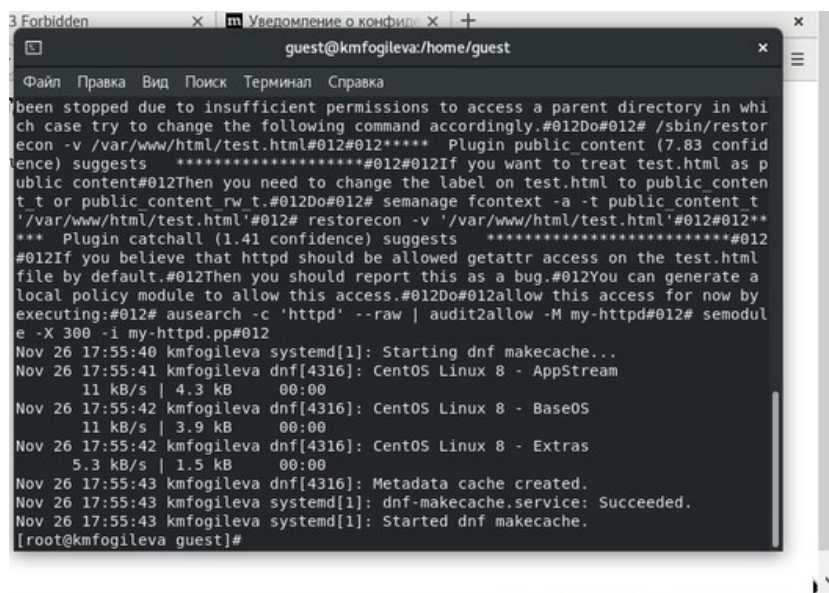


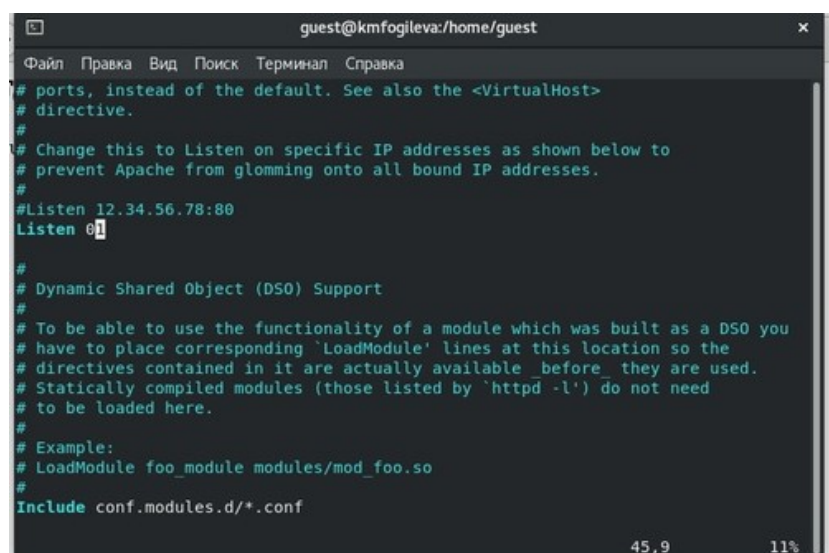
Figure 3.12: Проверка



```
3 Forbidden x m Уведомление о конфи... x +
guest@kmfogleva:/home/guest
Файл Правка Вид Поиск Терминал Справка
been stopped due to insufficient permissions to access a parent directory in whi
ch case try to change the following command accordingly.#012Do#012# /sbin/restor
econ -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confid
ence) suggests *****#012#012If you want to treat test.html as p
ublic content#012Then you need to change the label on test.html to public conten
t 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# semodul
e -X 300 -i my-httpd.pp#012
Nov 26 17:55:40 kmfogleva systemd[1]: Starting dnf makecache...
Nov 26 17:55:41 kmfogleva dnf[4316]: CentOS Linux 8 - AppStream
11 kB/s | 4.3 kB 00:00
Nov 26 17:55:42 kmfogleva dnf[4316]: CentOS Linux 8 - BaseOS
11 kB/s | 3.9 kB 00:00
Nov 26 17:55:42 kmfogleva dnf[4316]: CentOS Linux 8 - Extras
5.3 kB/s | 1.5 kB 00:00
Nov 26 17:55:43 kmfogleva dnf[4316]: Metadata cache created.
Nov 26 17:55:43 kmfogleva systemd[1]: dnf-makecache.service: Succeeded.
Nov 26 17:55:43 kmfogleva systemd[1]: Started dnf makecache.
[root@kmfogleva guest]#
```

Figure 3.13: Просмотр системного лог-файла

13. Попробовала запустить веб-сервер Араче на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf нашла строчку Listen 80 и заменила её на Listen 81.(рис. 3.14).



```
guest@kmfogleva:/home/guest
Файл Правка Вид Поиск Терминал Справка
# 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

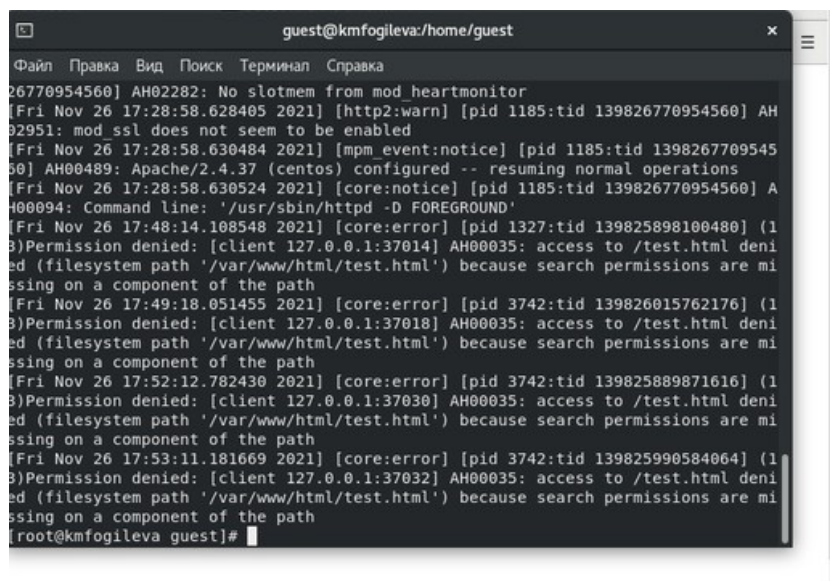
45,9 11%
```

Figure 3.14: Изменение порта 80 на 81

14. Проанализировала лог-файлы. Просмотрела файлы /var/log/http/error_log, /var/log/http/access_log и /var/log/audit/audit.log. (рис. 3.15), (рис. 3.16), (рис. 3.17), (рис. 3.18).

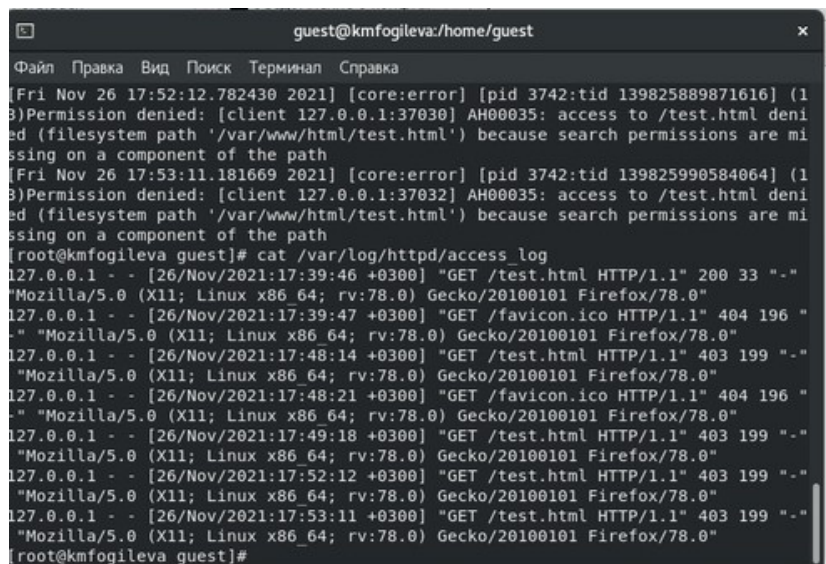
```
[root@kmfogleva guest]# tail -n1 /var/log/message
tail: невозможно открыть '/var/log/message' для чтения: Нет такого файла или каталога
[root@kmfogleva guest]# tail -n1 /var/log/messages
Nov 26 17:55:43 kmfogleva systemd[1]: Started dnf makecache.
[root@kmfogleva guest]#
```

Figure 3.15: Анализ лог-файла



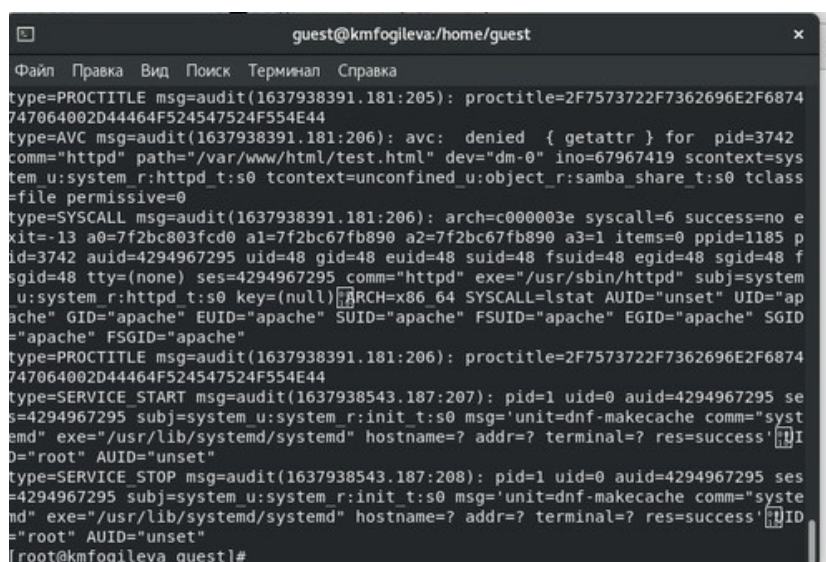
```
guest@kmfogleva:/home/guest
Файл Правка Вид Поиск Терминал Справка
26770954560] AH02282: No slotmem from mod_heartbeat
[Fri Nov 26 17:28:58.628405 2021] [http2:warn] [pid 1185:tid 139826770954560] AH02951: mod_ssl does not seem to be enabled
[Fri Nov 26 17:28:58.630484 2021] [mpm_event:notice] [pid 1185:tid 139826770954560] AH00489: Apache/2.4.37 (centos) configured -- resuming normal operations
[Fri Nov 26 17:28:58.630524 2021] [core:notice] [pid 1185:tid 139826770954560] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Fri Nov 26 17:48:14.108548 2021] [core:error] [pid 1327:tid 139825898100480] (13)Permission denied: [client 127.0.0.1:37014] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Fri Nov 26 17:49:18.051455 2021] [core:error] [pid 3742:tid 139826015762176] (13)Permission denied: [client 127.0.0.1:37018] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Fri Nov 26 17:52:12.782430 2021] [core:error] [pid 3742:tid 139825889871616] (13)Permission denied: [client 127.0.0.1:37030] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Fri Nov 26 17:53:11.181669 2021] [core:error] [pid 3742:tid 139825990584064] (13)Permission denied: [client 127.0.0.1:37032] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[root@kmfogleva guest]#
```

Figure 3.16: Просмотр файла /var/log/http/access_log



```
guest@kmfogleva:/home/guest
Файл Правка Вид Поиск Терминал Справка
[Fri Nov 26 17:52:12.782430 2021] [core:error] [pid 3742:tid 139825889871616] (1
3)Permission denied: [client 127.0.0.1:37030] AH00035: access to /test.html deni
ed (filesystem path '/var/www/html/test.html') because search permissions are mi
ssing on a component of the path
[Fri Nov 26 17:53:11.181669 2021] [core:error] [pid 3742:tid 139825990584064] (1
3)Permission denied: [client 127.0.0.1:37032] AH00035: access to /test.html deni
ed (filesystem path '/var/www/html/test.html') because search permissions are mi
ssing on a component of the path
[root@kmfogleva guest]# cat /var/log/httpd/access_log
127.0.0.1 - - [26/Nov/2021:17:39:46 +0300] "GET /test.html HTTP/1.1" 200 33 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [26/Nov/2021:17:39:47 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "
" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [26/Nov/2021:17:48:14 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [26/Nov/2021:17:48:21 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "
" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [26/Nov/2021:17:49:18 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [26/Nov/2021:17:52:12 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [26/Nov/2021:17:53:11 +0300] "GET /test.html HTTP/1.1" 403 199 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
[root@kmfogleva guest]#
```

Figure 3.17: Просмотр файла /var/log/http/error_log



```
guest@kmfogleva:/home/guest
Файл Правка Вид Поиск Терминал Справка
type=PROCTITLE msg=audit(1637938391.181:205): proctitle=2F7573722F7362696E2F6874
747064002D44464F524547524F554E44
type=AVC msg=audit(1637938391.181:206): avc: denied { getattr } for pid=3742
comm="httpd" path="/var/www/html/test.html" dev="dm-0" ino=67967419 scontext=sys
tem_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:samba_share_t:s0 tclass
=file permissive=0
type=SYSCALL msg=audit(1637938391.181:206): arch=c000003e syscall=6 success=no e
xit=-13 a0=7f2bc803fcd0 a1=7f2bc67fb890 a2=7f2bc67fb890 a3=1 items=0 ppid=1185 p
id=3742 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=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"
type=PROCTITLE msg=audit(1637938391.181:206): proctitle=2F7573722F7362696E2F6874
747064002D44464F524547524F554E44
type=SERVICE_START msg=audit(1637938543.187:207): pid=1 uid=0 auid=4294967295 se
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="syste
md" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' ID
="root" AUID="unset"
type=SERVICE_STOP msg=audit(1637938543.187:208): pid=1 uid=0 auid=4294967295 ses
s=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=dnf-makecache comm="syste
md" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' ID
="root" AUID="unset"
[root@kmfogleva guest]#
```

Figure 3.18: Просмотр файла var/log/audit/audit.log

15. Выполнила команду: `semanage port -a -t http_port_t -p tcp 81`. После это-
го проверила список портов командой: `semanage port -l | grep http_port_t`.
Убедилась, что порт 81 появился в списке. (рис. 3.19).

```

="root" AUID="unset"
[root@kmfogleva guest]# semanage port -a -t http_port_t -p tcp 81
bash: semanage: команда не найдена...
[root@kmfogleva guest]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@kmfogleva guest]# 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@kmfogleva guest]#

```

Figure 3.19: Выполнение и проверка

16. Вернула контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`:
`chcon -t httpd_sys_content_t /var/www/html/test.html`. После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Увидели содержимое файла — слово «test». (рис. 3.20), (рис. 3.21).

```

http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus http_port_t   tcp      5988
[root@kmfogleva guest]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@kmfogleva guest]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 ноя 25 16:59 /var/www/html/test.html
[root@kmfogleva guest]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@kmfogleva guest]#

```

Figure 3.20: Возвращение контекста

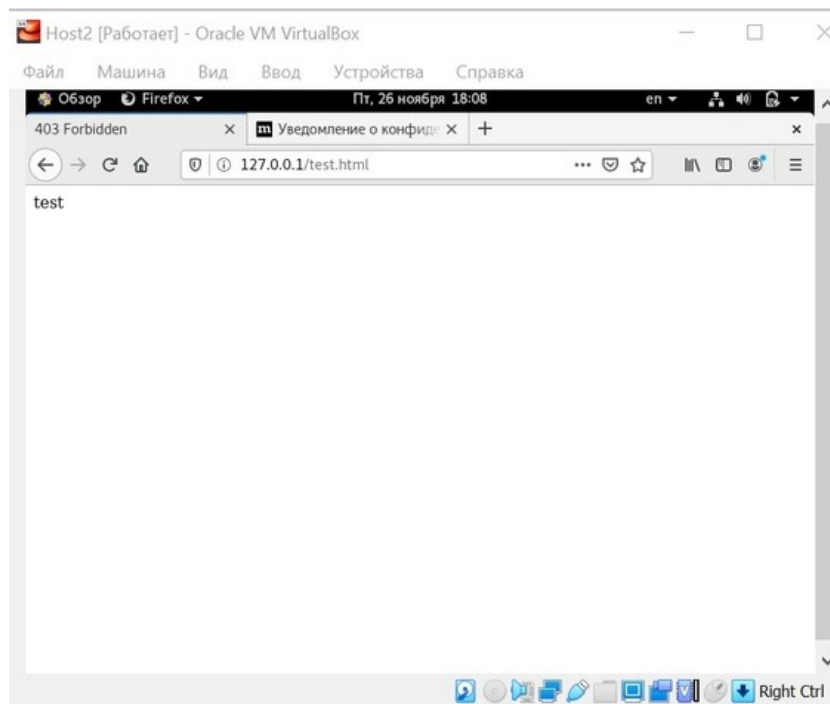


Figure 3.21: Получение доступа к файлу через браузер

17. Исправила обратно конфигурационный файл apache, вернув Listen 80. (рис. 3.22).



Figure 3.22: Исправление конфигурационного файл apache

18. Удалила привязку http_port_t к 81 порту. (рис. 3.23).

```

root@kmfogleva guest]# ls -Z /var/www/html/test.html
nconfined u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
root@kmfogleva guest]# vim /etc/httpd/conf/httpd.conf
root@kmfogleva guest]# semanage port -d -t http_port_t -p tcp 81
valueError: Порт tcp/81 определен на уровне политики и не может быть удален
root@kmfogleva guest]# rm /var/www/html/test.html
m: удалить обычный файл '/var/www/html/test.html'? y
root@kmfogleva guest]#

```

Figure 3.23: Удаление привязки http_port_t к 81 порту

19. Удалила файл /var/www/html/test.html. (рис. 3.24).

```

root@kmfogleva guest]# ls -Z /var/www/html/test.html
nconfined u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
root@kmfogleva guest]# vim /etc/httpd/conf/httpd.conf
root@kmfogleva guest]# semanage port -d -t http_port_t -p tcp 81
valueError: Порт tcp/81 определен на уровне политики и не может быть удален
root@kmfogleva guest]# rm /var/www/html/test.html
m: удалить обычный файл '/var/www/html/test.html'? y
root@kmfogleva guest]#

```

Figure 3.24: Удаление файла /var/www/html/test.html

4 Выводы

На основе проделанной работы развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinx на практике совместно с веб-сервером Apache.