

## **Лабораторная работа N° 6**

Информационная безопасность

Леон Фернандо Хосе Фернандо | НПМбд02-20

## Содержание

1 Цель работы .....	4
2 Теоретическое введение .....	4
3 Выполнение лабораторной работы .....	4
3.1 Создание программы.....	Ошибка! Закладка не определена.
3.2 Исследование Sticky-бита .....	Ошибка! Закладка не определена.
4 Выводы .....	10
5 Список Литературы .....	10

## Список иллюстраций

Рисунок 1. Предварительная подготовка .....	Ошибка! Закладка не определена.
Рисунок 2. Команда “whereis” .....	Ошибка! Закладка не определена.
Рисунок 3. Вход в систему и создание программы .....	Ошибка! Закладка не определена.
Рисунок 4. Код программы simpleid.c .....	Ошибка! Закладка не определена.
Рисунок 5. Компиляция и выполнение программы simpleid .....	Ошибка! Закладка не определена.
Рисунок 6. Усложнение программы .....	Ошибка! Закладка не определена.
Рисунок 7. Переименование программы в simpleid2.c .....	Ошибка! Закладка не определена.
Рисунок 8. Компиляция и выполнение программы simpleid2 .....	Ошибка! Закладка не определена.
Рисунок 9. Установка новых атрибутов (SetUID) .....	Ошибка! Закладка не определена.
Рисунок 10. Запуск simpleid2 после установки SetUID .....	Ошибка! Закладка не определена.
Рисунок 11. Запуск simpleid2 после установки SetGID .....	Ошибка! Закладка не определена.
Рисунок 12. Код программы readfile.c .....	Ошибка! Закладка не определена.
Рисунок 13. Смена владельца и прав доступа у файла readfile.c .....	Ошибка! Закладка не определена.
Рисунок 14. Запуск программы readfile .....	Ошибка! Закладка не определена.
Рисунок 15. Создание файла file01.txt .....	Ошибка! Закладка не определена.
Рисунок 16. Попытка выполнить действия над файлом file01.txt от имени пользо. ....	Ошибка!
<b>Закладка не определена.</b>	
Рисунок 17. Удаление атрибута t (Sticky-бита) .....	Ошибка! Закладка не определена.
Рисунок 18. Возвращение атрибута t (Sticky-бита) .....	Ошибка! Закладка не определена.

## 1 Цель работы

Совершенствуйте навыки администрирования ОС Linux, приобретайте начальный практический опыт работы с технологией SELinux и оценивайте функциональность SELinux на практике в сочетании с веб-сервером Apache.

## 2 Теоретическое введение

SELinux (Security-Enhanced Linux) обеспечивает усиление защиты путем внесения изменений как на уровне ядра, так и на уровне пространства пользователя, что превращает ее в действительно «непробиваемую» операционную систему. Впервые эта система появилась в четвертой версии CentOS, а в 5 и 6 версии реализация была существенно дополнена и улучшена.

SELinux имеет три основных режим работы:

- 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.

Политика SELinux определяет доступ пользователей к ролям, доступ ролей к доменам и доступ доменов к типам. Контекст безопасности — все атрибуты SELinux — роли, типы и домены.

Apache — это свободное программное обеспечение, с помощью которого можно создать веб-сервер. Данный продукт возник как доработанная версия другого HTTP-клиента от национального центра суперкомпьютерных приложений (NCSA).

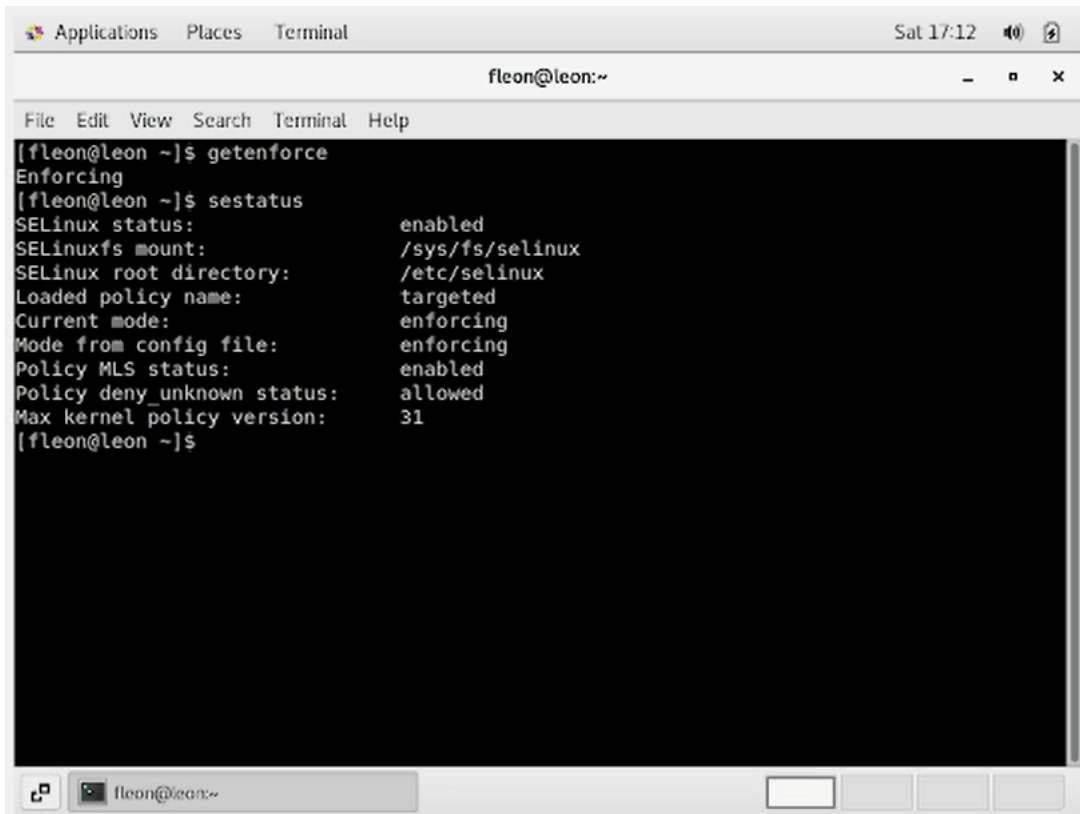
Для чего нужен Apache сервер:

- чтобы открывать динамические PHP-страницы,
- для распределения поступающей на сервер нагрузки,
- для обеспечения отказоустойчивости сервера,
- чтобы потренироваться в настройке сервера и запуске PHP-скриптов.

Apache является кроссплатформенным ПО и поддерживает такие операционные системы, как Linux, BSD, MacOS, Microsoft, BeOS и другие.

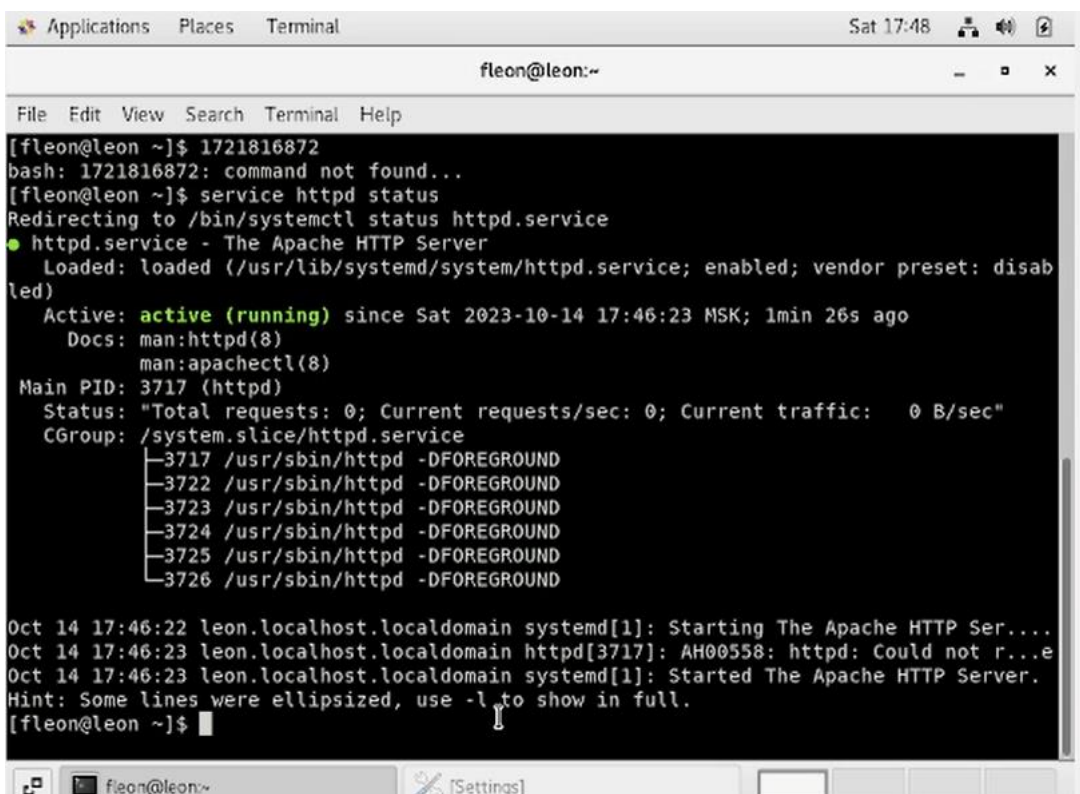
## 3 Выполнение лабораторной работы

Вошел в систему под своей учетной записью и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд “getenforce” и “sestatus”

A terminal window titled 'fleon@leon:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The user has entered the command 'getenforce' which returns 'Enforcing'. Then they enter 'sestatus' which displays the following SELinux status: 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.

```
[fleon@leon ~]$ getenforce
Enforcing
[fleon@leon ~]$ 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
[fleon@leon ~]$
```

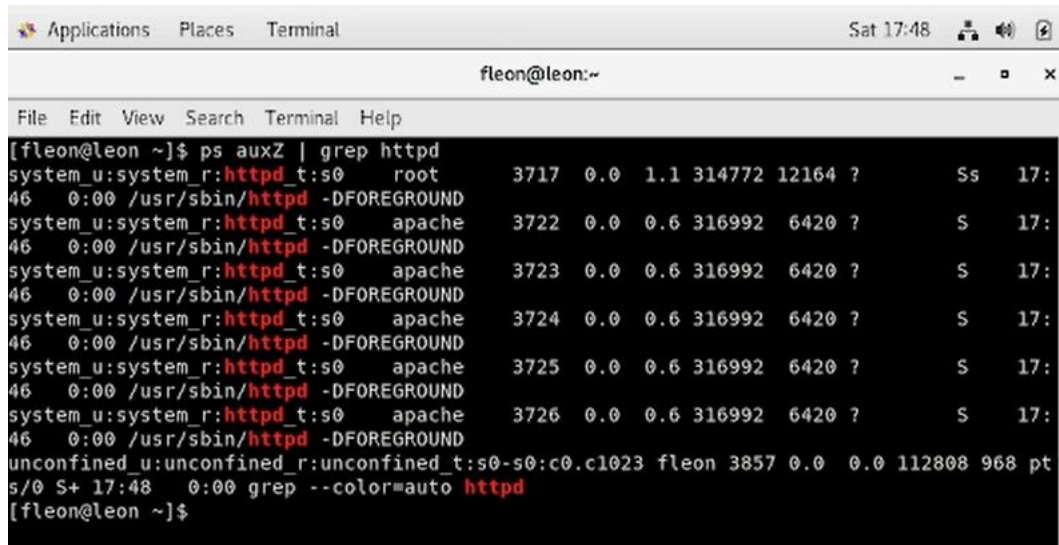
Обратился с помощью браузера к веб-серверу, запущенному на моем компьютере, и убедилась, что последний работает с помощью команды "service httpd status"

A terminal window titled 'fleon@leon:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The user enters a command that is not found, then 'service httpd status'. The output shows that httpd.service is active (running) and provides details about its configuration, PID, status, and CGroup. At the bottom, there are system logs indicating the service was started successfully.

```
[fleon@leon ~]$ 1721816872
bash: 1721816872: command not found...
[fleon@leon ~]$ 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 Sat 2023-10-14 17:46:23 MSK; 1min 26s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 3717 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
    CGroup: /system.slice/httpd.service
            └─3717 /usr/sbin/httpd -DFOREGROUND
              └─3722 /usr/sbin/httpd -DFOREGROUND
                └─3723 /usr/sbin/httpd -DFOREGROUND
                  └─3724 /usr/sbin/httpd -DFOREGROUND
                    └─3725 /usr/sbin/httpd -DFOREGROUND
                      └─3726 /usr/sbin/httpd -DFOREGROUND

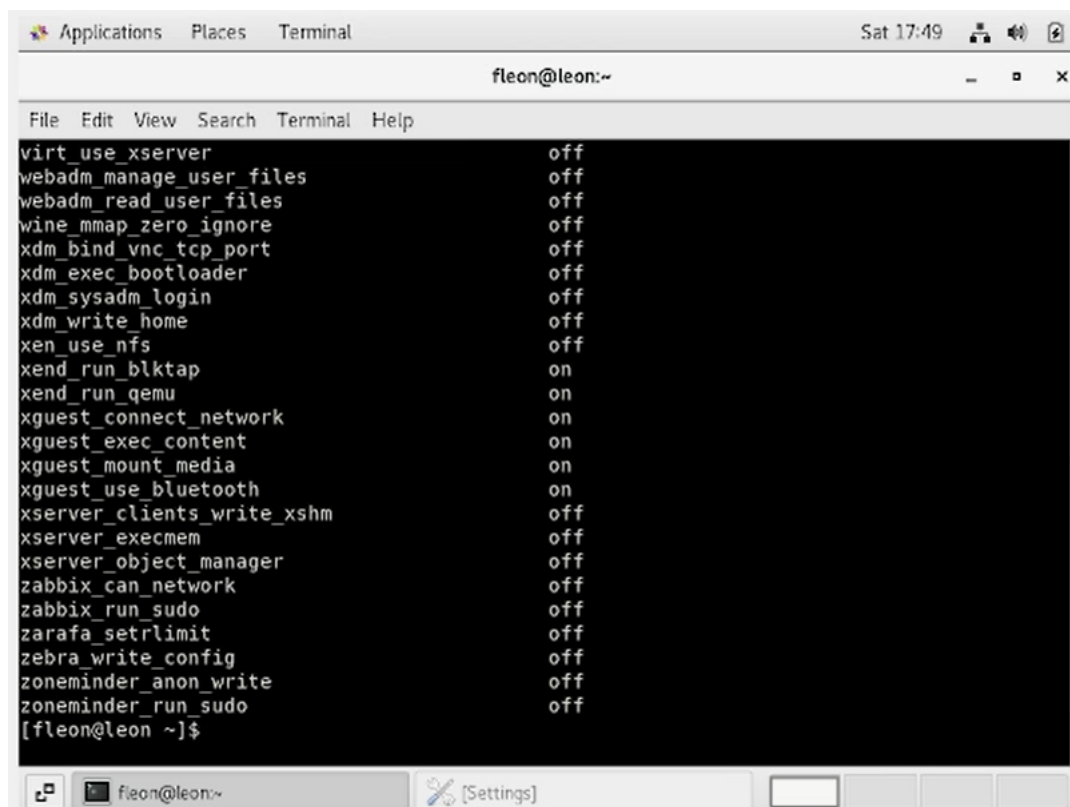
Oct 14 17:46:22 leon.localhost.localdomain systemd[1]: Starting The Apache HTTP Ser....
Oct 14 17:46:23 leon.localhost.localdomain httpd[3717]: AH00558: httpd: Could not r...e
Oct 14 17:46:23 leon.localhost.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[fleon@leon ~]$
```

С помощью команды “ps auxZ | grep httpd” определил контекст безопасности веб-сервера Apache - httpd\_t



```
[fleon@leon ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      3717  0.0  1.1 314772 12164 ?        Ss   17:
46   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3722  0.0  0.6 316992  6420 ?        S    17:
46   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3723  0.0  0.6 316992  6420 ?        S    17:
46   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3724  0.0  0.6 316992  6420 ?        S    17:
46   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3725  0.0  0.6 316992  6420 ?        S    17:
46   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  3726  0.0  0.6 316992  6420 ?        S    17:
46   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 fleon 3857  0.0  0.0 112808  968 pt
s/0 S+ 17:48   0:00 grep --color=auto httpd
[fleon@leon ~]$
```

Посмотрел текущее состояние переключателей SELinux для Apache с помощью команды “sestatus -bigrep httpd”, многие из переключателей находятся в положении “off”



```
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
xguest_connect_network          on
xguest_exec_content             on
xguest_mount_media              on
xguest_use_bluetooth            on
xserver_clients_write_xshm       off
xserver_execmem                 off
xserver_object_manager          off
zabbix_can_network              off
zabbix_run_sudo                 off
zafa_setrlimit                  off
zebra_write_config              off
zoneminder_anon_write           off
zoneminder_run_sudo             off
[fleon@leon ~]$
```

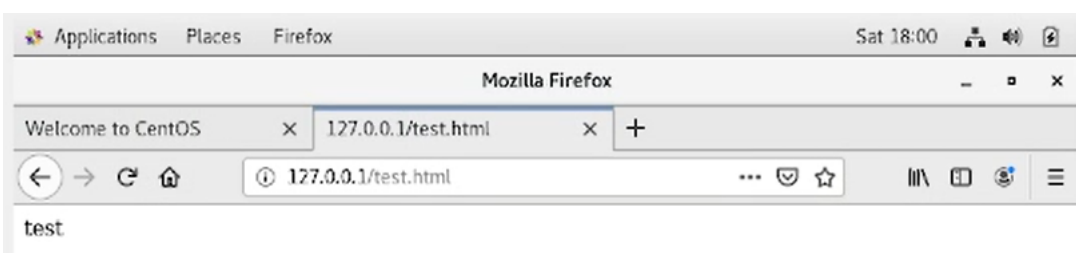
```
Applications Places Terminal Sat 17:50
root@leon:~
File Edit View Search Terminal Help
[fleon@leon ~]$ ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[fleon@leon ~]$ su -
Password:
Last login: Sat Oct 7 02:43:37 MSK 2023 on pts/1
[root@leon ~]#
```

Я использовал команду "ls -lZ /var/www" для просмотра файлов и подкаталогов, расположенных в каталоге /var/www. Используя команду "ls -lZ /var/www/html", я определил, что в этом каталоге нет файлов. Только владелец/суперпользователь имеет привилегию создавать файлы в каталоге /var/www/html.

```
Applications Places Terminal Sat 17:53
fleon@leon:~
File Edit View Search Terminal Help
[fleon@leon ~]$ 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
[fleon@leon ~]$ su -
Password:
Last login: Sat Oct 7 02:43:37 MSK 2023 on pts/1
[root@leon ~]# touch /var/www/html/test.html
[root@leon ~]# nano /var/www/html/test.html
[root@leon ~]# cat /var/www/html/test.html
<html>
<body>test</body>
</html>

[root@leon ~]# su - fleon
Last login: Sat Oct 14 17:11:28 MSK 2023 on :0
[fleon@leon ~]$
```

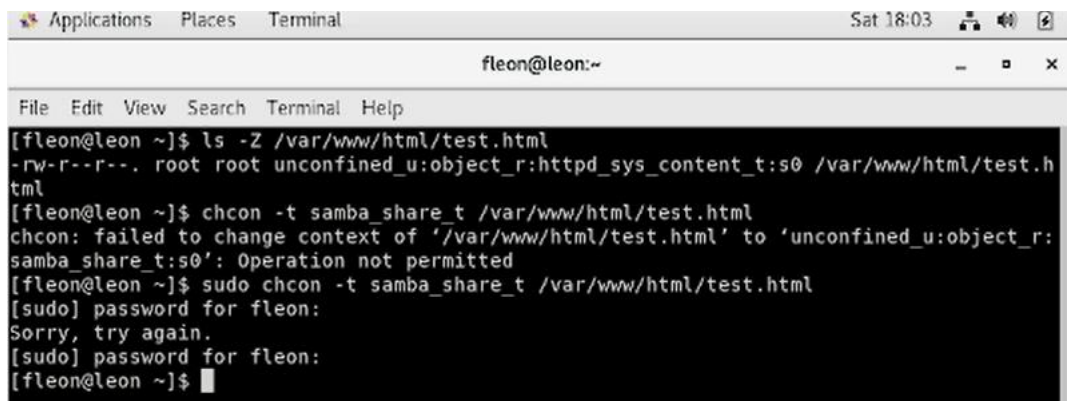
От имени суперпользователя создал html-файл /var/www/html/test.html. Контекст созданного файла - httpd\_sys\_content\_t. Обратился к файлу через веб-сервер, введя в браузере адрес "http://127.0.0.1/test.html". Файл был успешно отображен.



Изучив справочную страницу "man httpd\_selinux", я обнаружил, что для httpd определены следующие файловые контексты: httpd\_sys\_content\_t, httpd\_sys\_script\_exec\_t, httpd\_sys\_script\_ro\_t, httpd\_sys\_script\_rw\_t, httpd\_sys\_script\_ra\_t и httpd\_unconfined\_script\_exec\_trace.

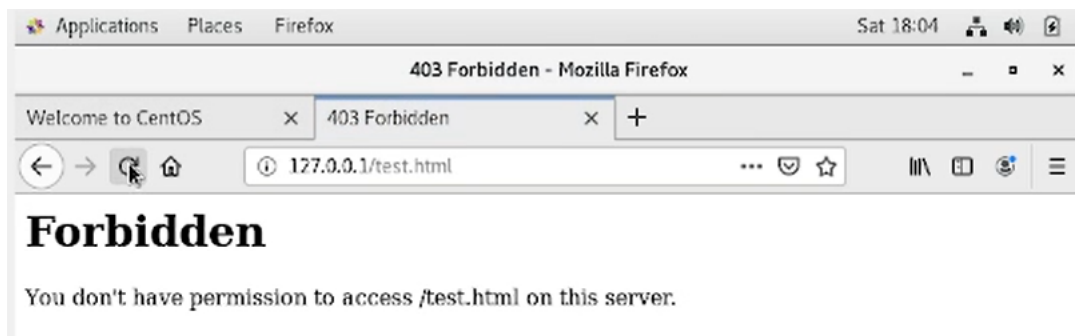
Контекст моего файла изначально был установлен в httpd\_sys\_content\_t (в этом случае содержимое должно быть доступно для всех скриптов httpd и самого демона httpd). Я

изменил контекст файла на `samba_share_t`, используя команду `"sudo chcon -t samba_share_t /var/www/html/test.html"` и убедился, что контекст был успешно изменен.



```
fleon@leon:~  
File Edit View Search Terminal Help  
[fleon@leon ~]$ ls -Z /var/www/html/test.html  
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[fleon@leon ~]$ chcon -t samba_share_t /var/www/html/test.html  
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:samba_share_t:s0': Operation not permitted  
[fleon@leon ~]$ sudo chcon -t samba_share_t /var/www/html/test.html  
[sudo] password for fleon:  
Sorry, try again.  
[sudo] password for fleon:  
[fleon@leon ~]$
```

Попробовал еще раз получить доступ к файлу через веб-сервер, введя в браузере адрес `"http://127.0.0.1/test.html"` и получила сообщение об ошибке (т.к. к установленному ранее контексту процесс `httpd` не имеет доступа)



С помощью команды `"ls -l /var/www/html/test.html"`, я подтвердил, что любой пользователь может прочитать этот файл. Я также просмотрел файл системного журнала веб-сервера Apache, используя команду `"sudo tail /var/log/messages"`, которая отображает ошибки.



```
Applications  Places  Terminal  Sat 18:05  fleon@leon:~
File Edit View Search Terminal Help
roubleshootd' (using servicehelper)
Oct 14 18:04:56 leon dbus[686]: [system] Successfully activated service 'org.fedoraproj
ect.Setroubleshootd'
Oct 14 18:04:56 leon setroubleshoot: failed to retrieve rpm info for /var/www/html/test
.html
Oct 14 18:04:56 leon setroubleshoot: SELinux is preventing httpd from getattr access on
the file /var/www/html/test.html. For complete SELinux messages run: sealert -l 32684b
64-51d5-494a-98a5-87b10a43bf70
Oct 14 18:04:56 leon python: SELinux is preventing httpd from getattr access on the fil
e /var/www/html/test.html.#012#012**** Plugin restorecon (92.2 confidence) suggests
*****#012#012If you want to fix the label. #012/var/www/html/test.h
tml default label should be httpd_sys_content_t.#012Then you can run restorecon. The ac
cess attempt may have been stopped due to insufficient permissions to access a parent d
irectory in which case try to change the following command accordingly.#012Do#012# /sbi
n/restorecon -v /var/www/html/test.html#012#012**** Plugin public_content (7.83 confi
dence) suggests *****#012#012If you want to treat test.html as public
content#012Then you need to change the label on test.html to public_content_t or public
_content_rw_t.#012Do#012# semanage fcontext -a -t public_content_t '/var/www/html/test.
html'#012# restorecon -v '/var/www/html/test.html'#012#012**** Plugin catchall (1.41
confidence) suggests *****#012#012If you believe that httpd shou
ld be allowed getattr access on the test.html file by default.#012Then you should repor
t this as a bug.#012You can generate a local policy module to allow this access.#012Do#
012allow this access for now by executing:#012# ausearch -c 'httpd' --raw | audit2allow
-M my-httpd#012# semodule -i my-httpd.pp#012
[fleon@leon ~]$
```

В файле /etc/httpd/conf/httpd.conf заменил строчку “Listen 80” на “Listen 81”, чтобы установить веб-сервер Apache на прослушивание TCP-порта 81

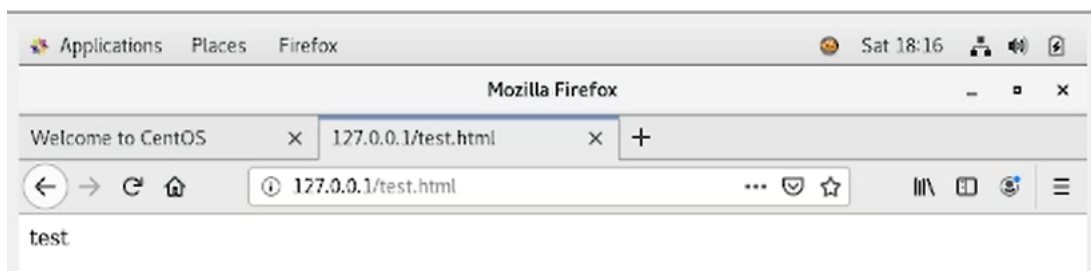
```
Applications  Places  Terminal  Sat 18:10  fleon@leon:~
File Edit View Search Terminal Help
[fleon@leon ~]$ systemctl restart httpd
[fleon@leon ~]$ tail -nl /var/log/messages
tail: l: invalid number of lines
[fleon@leon ~]$ tail -nl /var/log/messages
tail: cannot open '/var/log/messages' for reading: Permission denied
[fleon@leon ~]$ tail -nl /var/log/messages
tail: l: invalid number of lines
[fleon@leon ~]$
```

Перезапускаем веб-сервер Apache и анализирует лог-файлы командой “tail -nl /var/log/messages”

```
Applications  Places  Terminal  Sat 18:12  root@leon:~
File Edit View Search Terminal Help
[fleon@leon ~]$ su -
Password:
Last login: Sat Oct 14 17:50:38 MSK 2023 on pts/0
[root@leon ~]# 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@leon ~]# systemctl restart httpd
[root@leon ~]#
```

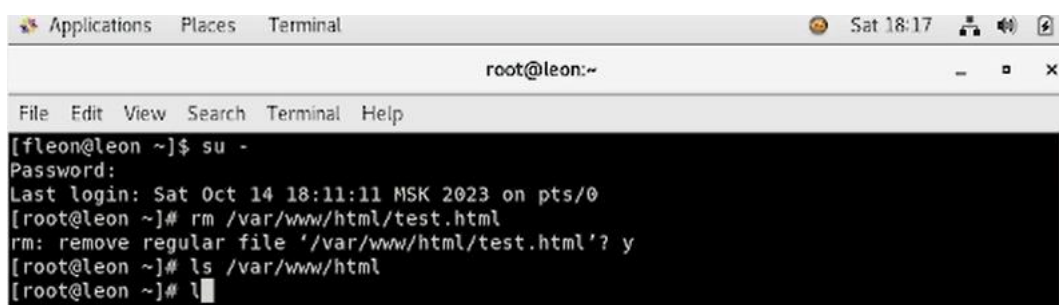
Просмотрел файлы “var/log/http/error\_log”, “/var/log/http/access\_log” и “/var/log/audit/audit.log” и выяснил, что запись появился в последнем файле

Выполнил команду “semanage port -a -t http\_port\_t -p tcp 81” и убедился, что порт TCP-81 установлен. Проверил список портов командой “semanage port -l | grep http\_port\_t”, убедился, что порт 81 есть в списке и запускаем веб-сервер Apache снова



Вернул контекст “httpd\_sys\_content\_t” файлу “/var/www/html/test.html” командой “chcon -t httpd\_sys\_content\_t /var/www/html/test.html” (рис. 3.16) и после этого попробовала получить доступ к файлу через веб-сервер, введя адрес “http://127.0.0.1:81/test.html”, в результате чего увидела содержимое файла - слово “test”

Я исправил конфигурационный файл Apache обратно на "Listen 80". Я попытался удалить привязку http\_port к порту 81, используя команду "semanage port -d -t http\_port\_t -p tcp 81", но поскольку этот порт определен на уровне политики, он не может быть удален. Удалил файл “/var/www/html/test.html” командой “rm /var/www/html/test.html”



## 4 Выводы

В ходе этой лабораторной работы я развил навыки администрирования ОС Linux, получил свое первое практическое представление о технологии SELinux и проверил функциональность SELinux на практике в сочетании с веб-сервером Apache.

## 5 Список Литературы

1. SELinux – описание и особенности работы с системой [Электронный ресурс]. URL: <https://habr.com/ru/company/kingservers/blog/209644/>.
2. Что такое Apache и зачем он нужен? [Электронный ресурс]. URL: <https://2domains.ru/support/vps-i-servery/shto-takoye-apache>.