

# Лабораторная работа № 6

---

Информационная безопасность

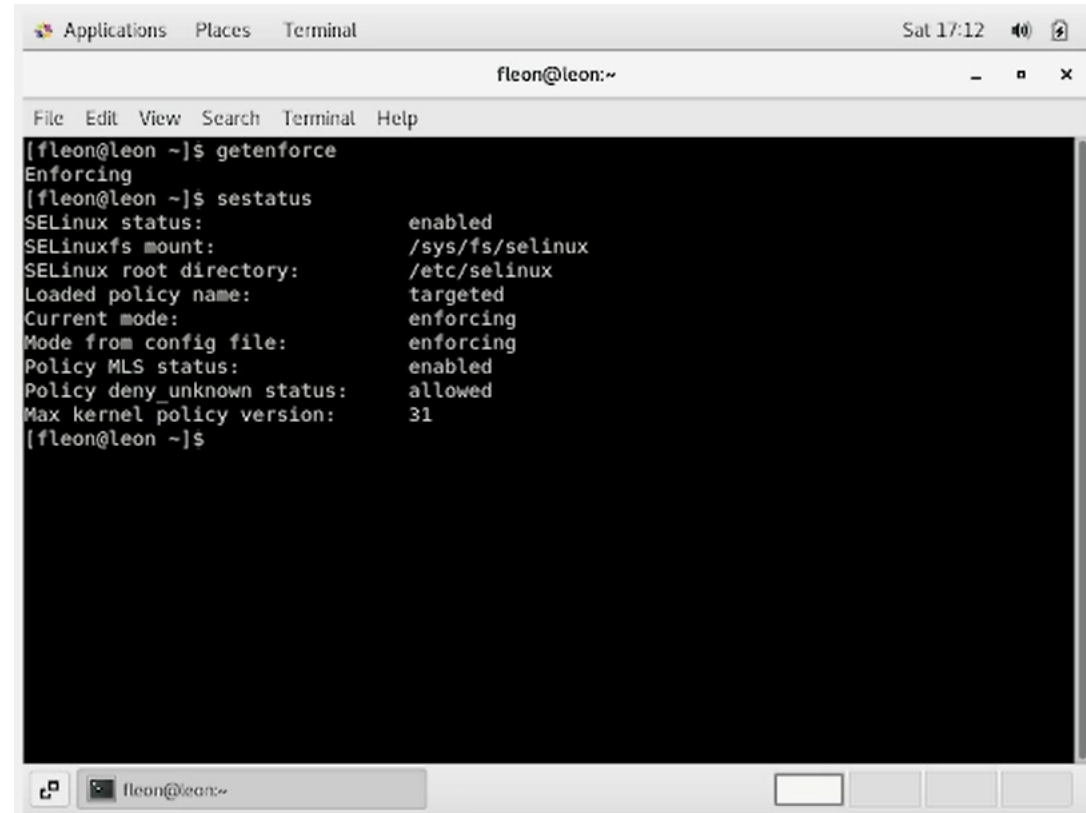
# Цель работы

---

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.

# Выполнение лабораторной работы

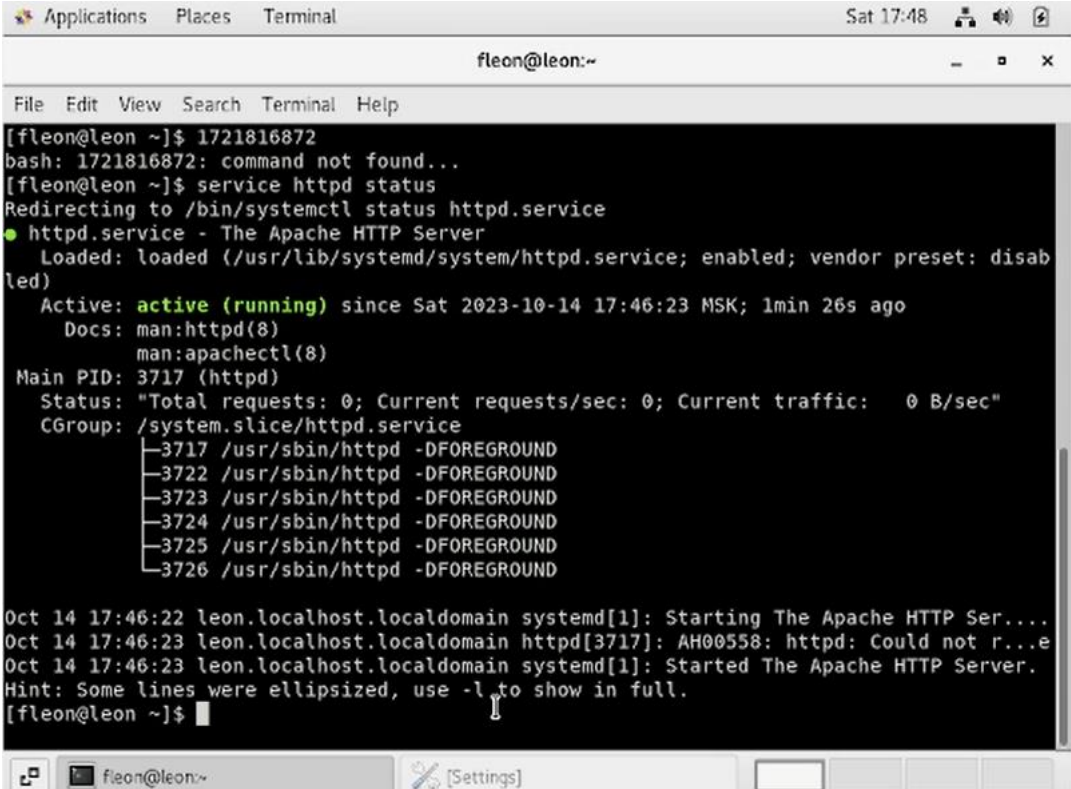
Вошел в систему под своей учетной записью и убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд “getenforce” и “sestatus”

A screenshot of a Linux terminal window. The window title bar shows 'Applications Places Terminal' on the left, 'Sat 17:12' and system icons on the right. The terminal itself has a title bar 'fleon@leon:~' and a menu bar 'File Edit View Search Terminal Help'. The terminal content shows the user 'fleon@leon' in the home directory '~' running two commands. First, 'getenforce' returns 'Enforcing'. Second, 'sestatus' returns a detailed status: SELinux status is 'enabled', SELinuxfs mount is '/sys/fs/selinux', SELinux root directory is '/etc/selinux', Loaded policy name is 'targeted', Current mode is 'enforcing', Mode from config file is 'enforcing', Policy MLS status is 'enabled', Policy deny\_unknown status is 'allowed', and Max kernel policy version is '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 ~]$
```

# Выполнение лабораторной работы

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

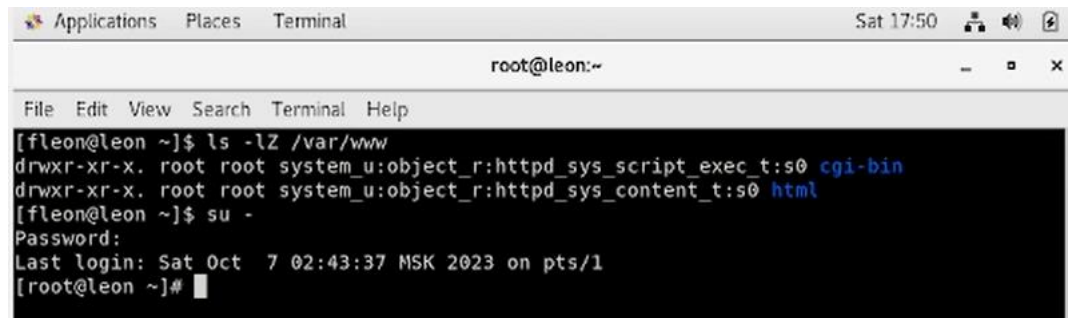


```
fleon@leon:~$ 1721816872
bash: 1721816872: command not found...
[fleon@leon ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (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

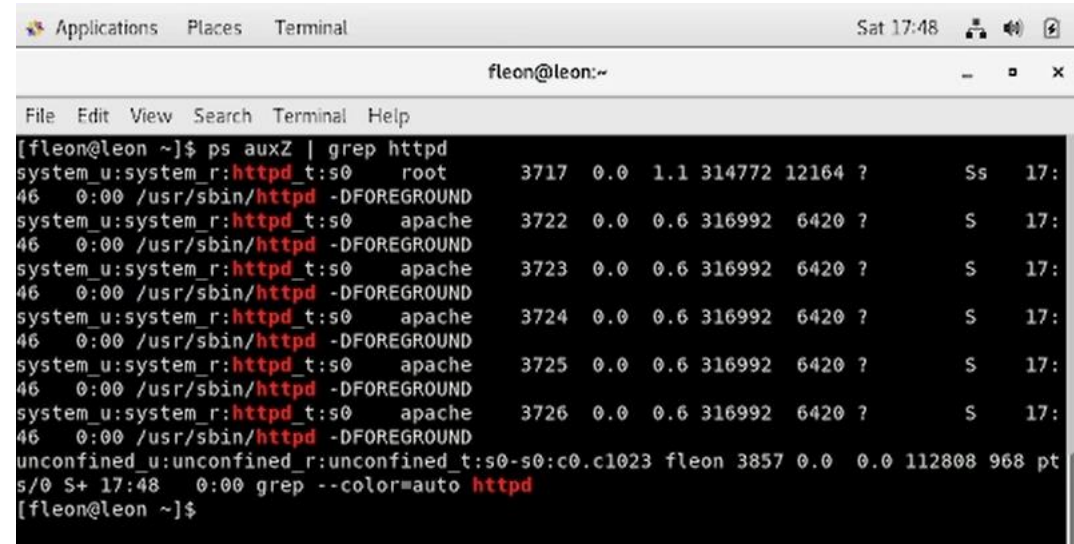
Oct 14 17:46:22 leon.localhost.localdomain systemd[1]: Starting The Apache HTTP Ser....
Oct 14 17:46:23 leon.localhost.localdomain httpd[3717]: AH00558: httpd: Could not r...e
Oct 14 17:46:23 leon.localhost.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use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

# Выполнение лабораторной работы

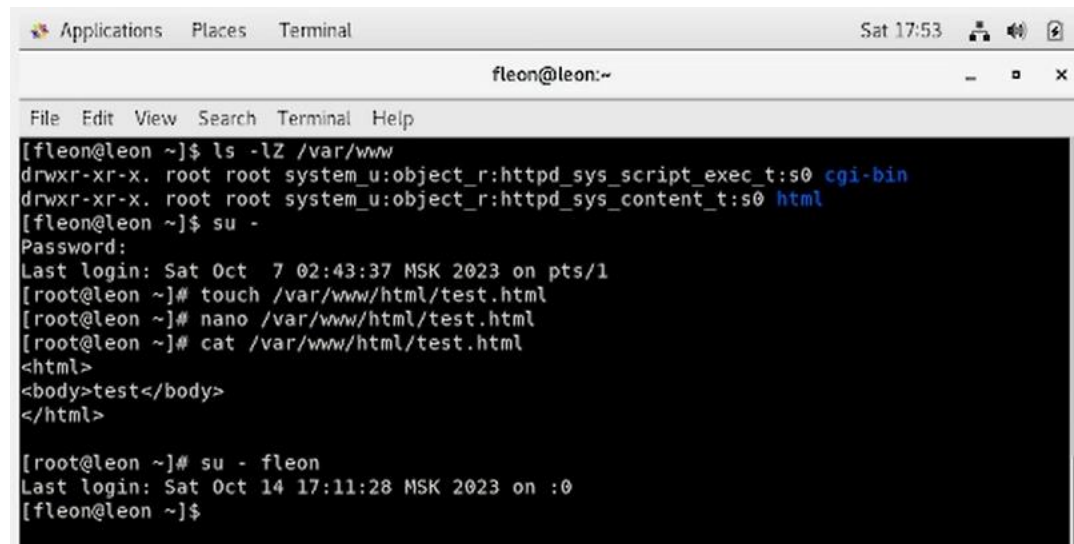
- С помощью команды "ps auxZ | grep httpd" определил контекст безопасности веб-сервера Apache - httpd\_t
- Я использовал команду "ls -lZ /var/www" для просмотра файлов и подкаталогов, расположенных в каталоге /var/www. Используя команду "ls -lZ /var/www/html", я определил, что в этом каталоге нет файлов.



```
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 ~]#
```



```
Applications  Places  Terminal  Sat 17:48
fleon@leon:~
File Edit View Search Terminal Help
[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 ~]$
```



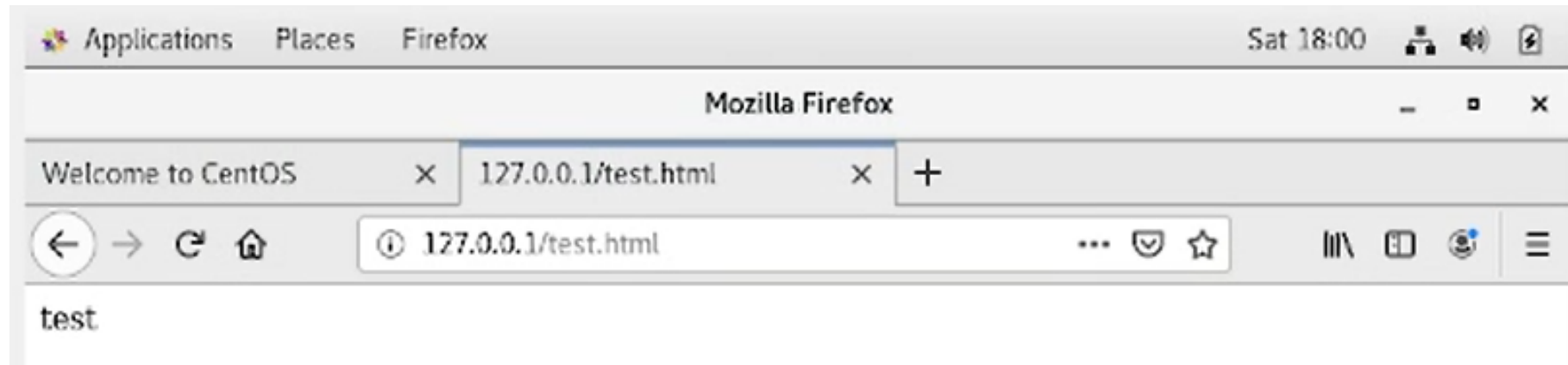
```
Applications  Places  Terminal  Sat 17:53
fleon@leon:~
File Edit View Search Terminal Help
[fleon@leon ~]$ ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[fleon@leon ~]$ su -
Password:
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 ~]$
```

# Выполнение лабораторной работы

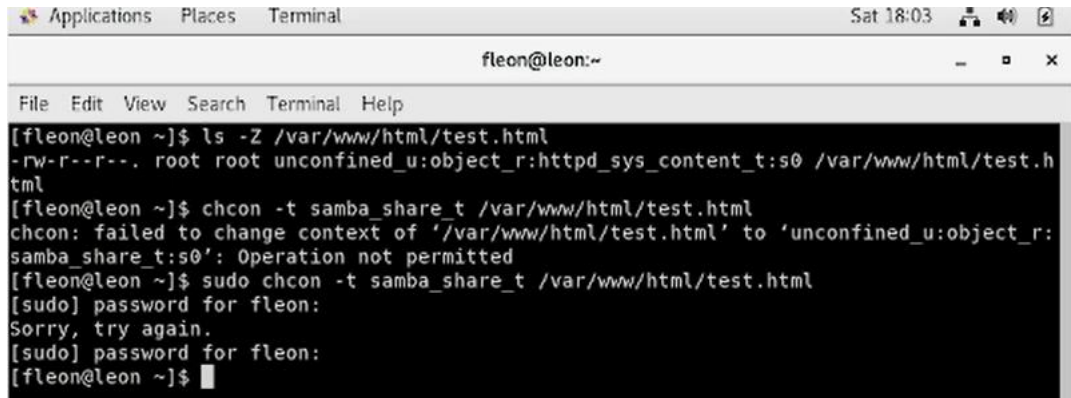
Обратился к файлу через веб-сервер, введя в браузере адрес “http://127.0.0.1/test.html”.

Файл был успешно отображен

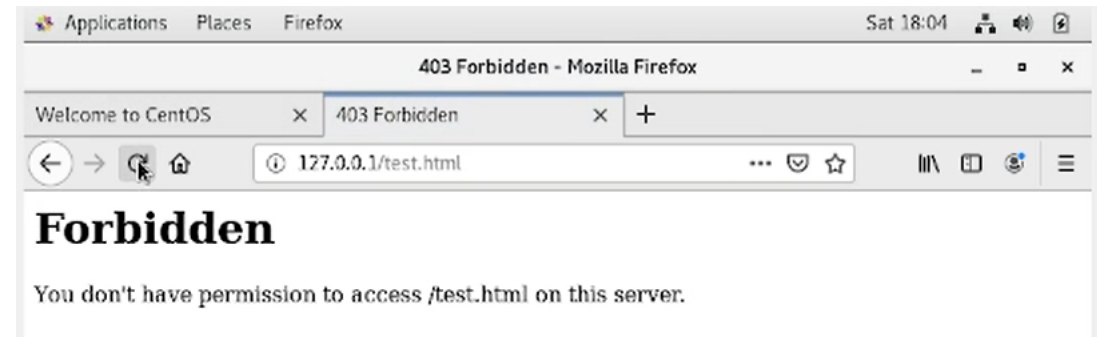


# Выполнение лабораторной работы

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.



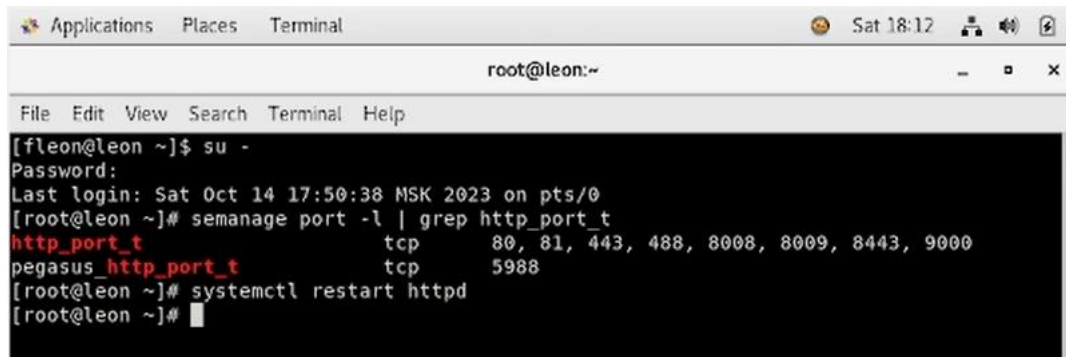
```
fleon@leon:~  
File Edit View Search Terminal Help  
[fleon@leon ~]$ ls -Z /var/www/html/test.html  
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[fleon@leon ~]$ chcon -t samba_share_t /var/www/html/test.html  
chcon: failed to change context of '/var/www/html/test.html'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



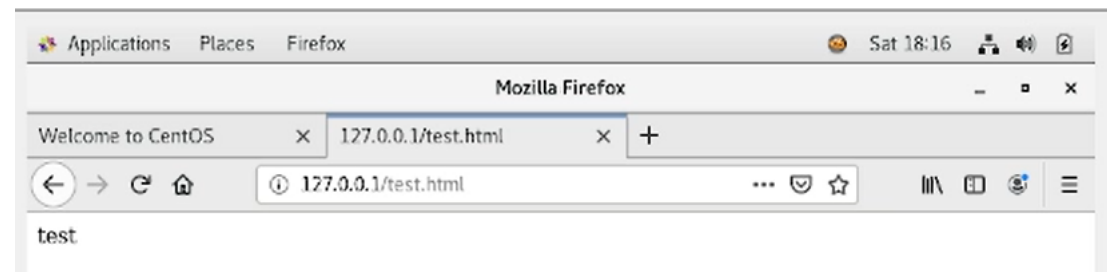
# Выполнение лабораторной работы

Перезапускаем веб-сервер Apache и анализирует лог-файлы командой “tail -n1 /var/log/messages”

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



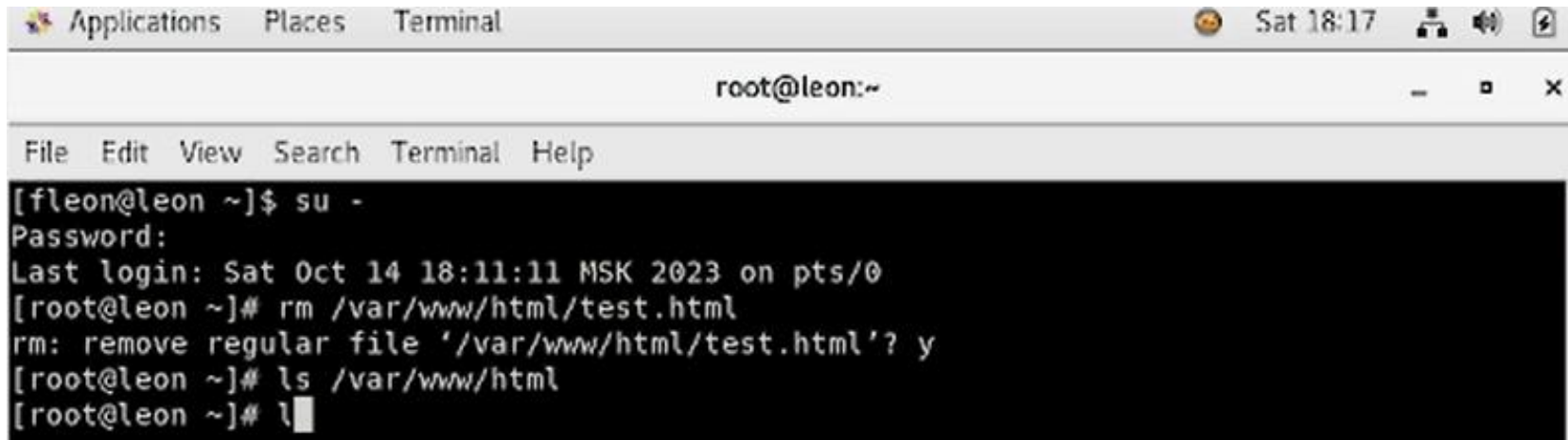
```
root@leon:~  
File Edit View Search Terminal Help  
[fleon@leon ~]$ su -  
Password:  
Last login: Sat Oct 14 17:50:38 MSK 2023 on pts/0  
[root@leon ~]# semanage port -l | grep http_port_t  
http_port_t            tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000  
pegasus_http_port_t    tcp      5988  
[root@leon ~]# systemctl restart httpd  
[root@leon ~]#
```





# Выполнение лабораторной работы

Удалил файл “/var/www/html/test.html” командой “rm /var/www/html/test.html”

A screenshot of a Linux terminal window. The window title bar shows 'Applications Places Terminal' and the system clock 'Sat 18:17'. The terminal prompt is 'root@leon:~'. The user has executed the command 'rm /var/www/html/test.html', and the output shows the file has been removed. The terminal also shows the user switching from a regular user to root using 'su -' and then listing the contents of the directory with 'ls /var/www/html'.

```
Applications Places Terminal Sat 18:17
root@leon:~
File Edit View Search Terminal Help
[flon@leon ~]$ su -
Password:
Last login: Sat Oct 14 18:11:11 MSK 2023 on pts/0
[root@leon ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@leon ~]# ls /var/www/html
[root@leon ~]# l
```

# 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.