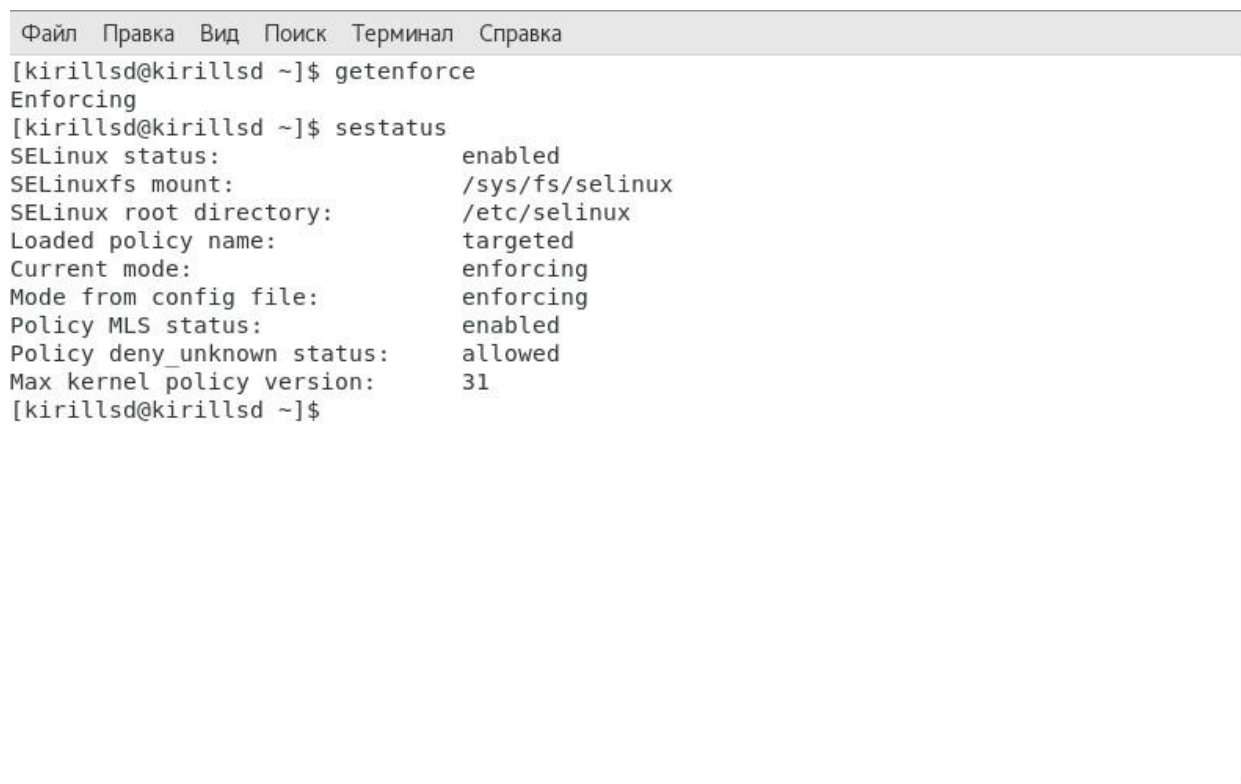


Лабораторная работа №6

Цель лабораторной работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Проверяем, что SELinux работает в режиме enforcing политики targeted.

A terminal window with a menu bar at the top containing 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows the execution of two commands: 'getenforce' and 'sestatus'. The output of 'getenforce' is 'Enforcing'. The output of 'sestatus' is a multi-line status report.

```
[kirillsd@kirillsd ~]$ getenforce
Enforcing
[kirillsd@kirillsd ~]$ 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
[kirillsd@kirillsd ~]$
```

getenforce и sestatus

Убеждаемся, что веб-браузер работает.

```
[kirillsd@kirillsd ~]$ 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 C6 2021-11-27 18:27:59 MSK; 1min 16s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 19666 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
    CGroup: /system.slice/httpd.service
            └─19666 /usr/sbin/httpd -DFOREGROUND
              └─19670 /usr/sbin/httpd -DFOREGROUND
                └─19671 /usr/sbin/httpd -DFOREGROUND
                  └─19672 /usr/sbin/httpd -DFOREGROUND
                    └─19673 /usr/sbin/httpd -DFOREGROUND
                      └─19674 /usr/sbin/httpd -DFOREGROUND

ноя 27 18:27:59 kirillsd.localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 27 18:27:59 kirillsd.localdomain httpd[19666]: AH00558: httpd: Could not rel...e
ноя 27 18:27:59 kirillsd.localdomain systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[kirillsd@kirillsd ~]$
```

↑

service

Найходим веб-сервер Apache в списке процессов

```
[kirillsd@kirillsd ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0      apache      14818  0.0  0.0 232524   948 ?        Ss
17  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      root       19666  0.0  0.0 230440   540 ?        Ss
27  0:01 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache     19670  0.0  0.0 232524   932 ?        S
27  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache     19671  0.0  0.1 232660  1836 ?        S
27  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache     19672  0.0  0.0 232524    64 ?        S
27  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache     19673  0.0  0.0 232524    64 ?        S
27  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache     19674  0.0  0.0 232660   820 ?        S
27  0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 kirillsd 19764 0.0  0.0 112
8 pts/0 R+ 22:01  0:00 grep --color=auto httpd
[kirillsd@kirillsd ~]$
```

Apache

Смотрим состояние переключателей SELinux для Apache

```
Файл  Правка  Вид  Поиск  Терминал  Справка
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
zarafa_setrlimit                off
zebra_write_config              off
zoneminder_anon_write           off
zoneminder_run_sudo             off
[kirillsd@kirillsd ~]$
```

SELinux

Определяем тип файлов и поддиректорий, находящихся в директории “/var/www”

```
[kirillsd@kirillsd ~]$ 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
[kirillsd@kirillsd ~]$ ls -lZ /var/www/html
[kirillsd@kirillsd ~]$
```

тип файлов

Создаем от имени суперпользователя html-файл “/var/www/html/test.html”

```
[kirillsd@kirillsd ~]$ ls -lZ /var/www/html
[kirillsd@kirillsd ~]$ su
Пароль:
[root@kirillsd kirillsd]# cd /var/www/html
[root@kirillsd html]# touch test.html
[root@kirillsd html]#
```

test.html

Содержание файла

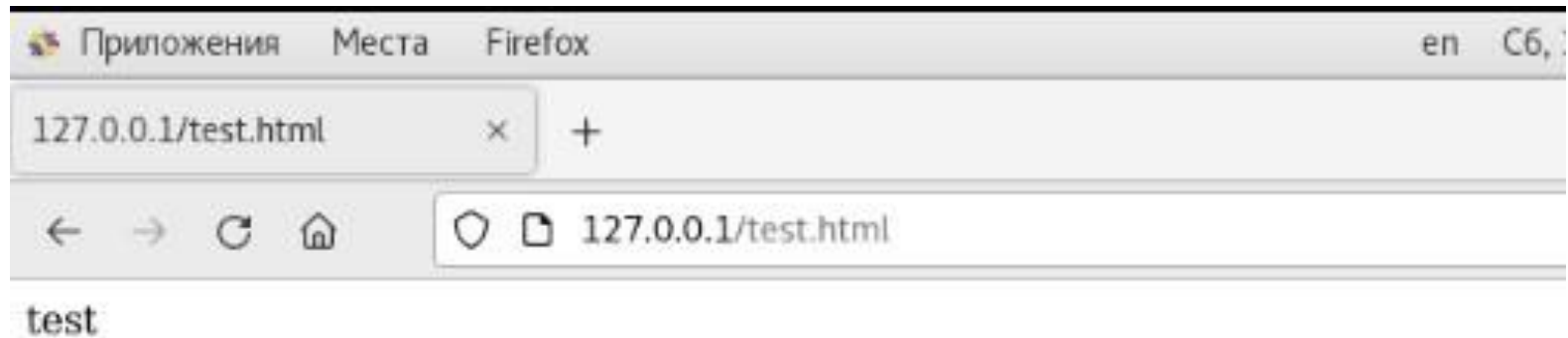


The image shows a screenshot of a text editor window. The title bar at the top contains the text '*test.html' and the file path '/var/www/html'. On the left side of the title bar is a button labeled 'Открыть' (Open) with a dropdown arrow, and on the right side is a button labeled 'Сохранить' (Save). The main editing area contains the following HTML code:

```
<html>  
<body>test</body>  
</html>
```

test.html

Вводим в браузере адрес
“http://127.0.0.1/test.html”



Браузер

Изучаем справку man httpd_selinux

```
Файл  Правка  Вид  Поиск  Терминал  Справка
HTTPD(8)                                     httpd                                     HTTPD(8)

NAME
    httpd - Apache Hypertext Transfer Protocol Server

SYNOPSIS
    httpd [ -d serverroot ] [ -f config ] [ -C directive ] [ -c directive ] [ -D
    parameter ] [ -e level ] [ -E file ] [ -k start|restart|graceful|stop|grace-
    ful-stop ] [ -R directory ] [ -h ] [ -l ] [ -L ] [ -S ] [ -t ] [ -v ] [ -V ]
    [ -X ] [ -M ] [ -T ]

    On Windows systems, the following additional arguments are available:

    httpd [ -k install|config|uninstall ] [ -n name ] [ -w ]

SUMMARY
    httpd is the Apache HyperText Transfer Protocol (HTTP) server program. It is
    designed to be run as a standalone daemon process. When used like this it
    will create a pool of child processes or threads to handle requests.

    In general, httpd should not be invoked directly, but rather should be
    invoked via apachectl on Unix-based systems or as a service on Windows NT,
    2000 and XP and as a console application on Windows 9x and ME.

Manual page httpd(8) line 1 (press h for help or q to quit)
```

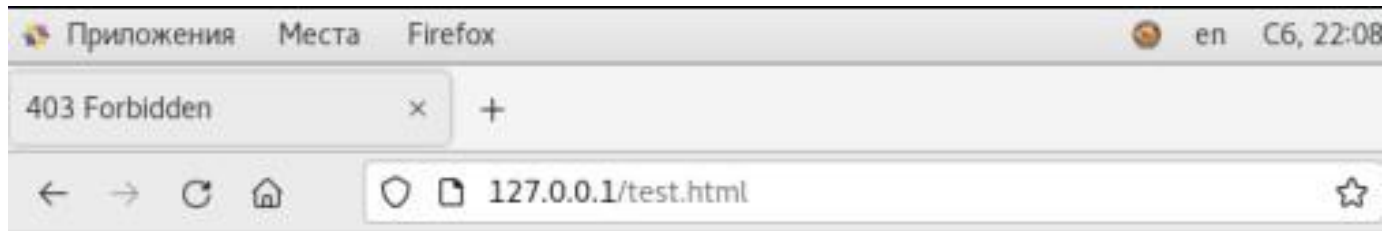
man httpd_selinux

Изменяем контекст файла “/var/www/html/test.html”

```
[root@kirillsd html]# chcon -t samba_share_t /var/www/html/test.html  
[root@kirillsd html]# ls -Z /var/www/html/test/html
```

Контекст файла

Попробуем ещё раз получить доступ к файлу



Forbidden

You don't have permission to access /test.html on this server.

simpleid2 и id

Выполняем перезапуск веб-сервера Apache

```
[root@kirillsd html]# sudo ststemctl reload httpd
sudo: ststemctl: command not found
[root@kirillsd html]# sudo systemctl reload httpd
[root@kirillsd html]# 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@kirillsd html]# tail -n1 /var/log/messages
Nov 27 22:16:22 kirillsd systemd: Reloaded The Apache HTTP Server.
[root@kirillsd html]# sudo systemctl restart httpd
[root@kirillsd html]# tail -n1 /var/log/messages
Nov 27 22:17:21 kirillsd systemd: Started The Apache HTTP Server.
[root@kirillsd html]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@kirillsd html]# 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@kirillsd html]#
```

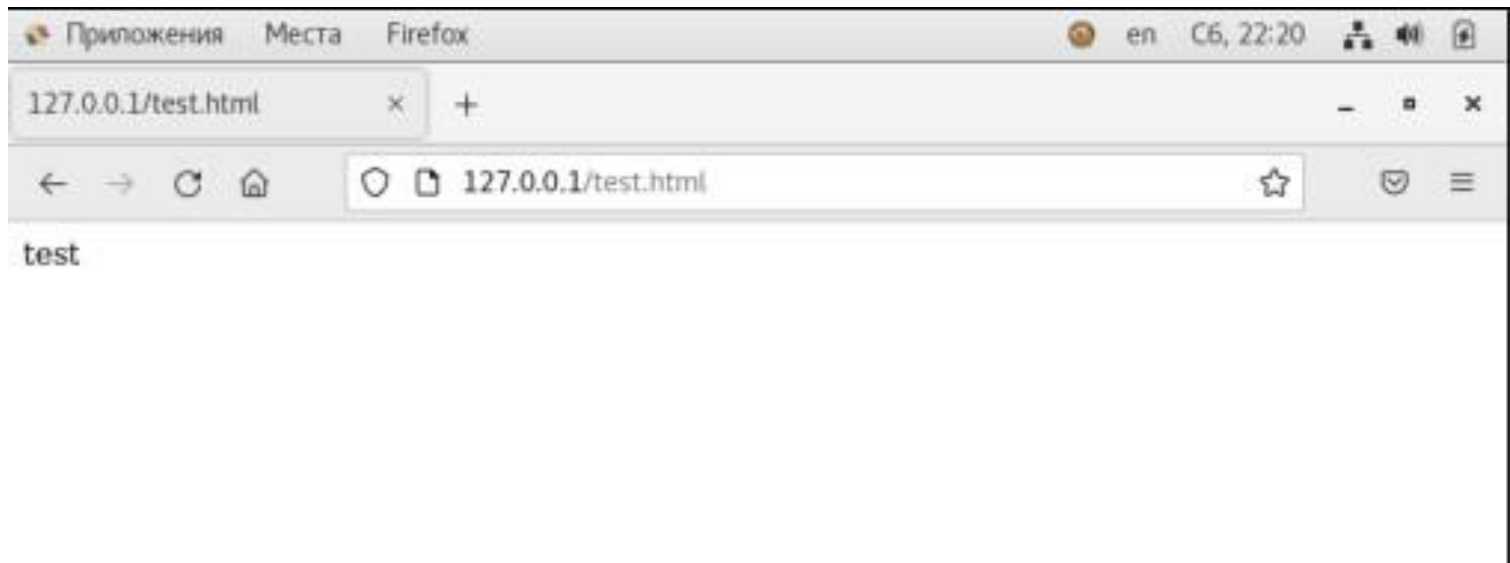
readfile.c

Выполняем команду “semanage port -a -t http_port_t -p tcp 81”

```
[root@kirillsd html]# 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@kirillsd html]#
```

semanage port

Верните контекст `httpd_sys_content__t` и
попытаемся получить доступ к файлу через
веб-сервер.



`httpd_sys_content_t`

Удаляем файл test.html: rm
“/var/www/html/test.html”

```
[root@kirillsd html]# rm test.html
rm: удалить обычный файл «test.html»? y
[root@kirillsd html]#
```

readfile.c

Вывод

В результате выполнения лабораторной работы мы развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux1. Проверили работу SELinux на практике совместно с веб-сервером Apache.