

# Лабораторная работа 6

Мандатное разграничение прав в Linux

Илья Валерьевич Фирстов

# Содержание

Цель работы	5
Задание	6
Теоретическое введение	7
Выполнение лабораторной работы	8
Выводы	13
Список литературы	14

# Список иллюстраций

1	SELinux работает в режиме enforcing политики targeted . . . .	8
2	service httpd status . . . . .	9
3	остояние переключателей SELinux . . . . .	9
4	Тип файлов в директории /var/www . . . . .	10
5	Отображение файла test.html . . . . .	10
6	Контекст test.html . . . . .	11
7	Ошибка доступа . . . . .	11
8	Просмотр логов . . . . .	12

## Список таблиц

## Цель работы

- с. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache

# Задание

Развить навыки администрирования ОС Linux

# Теоретическое введение

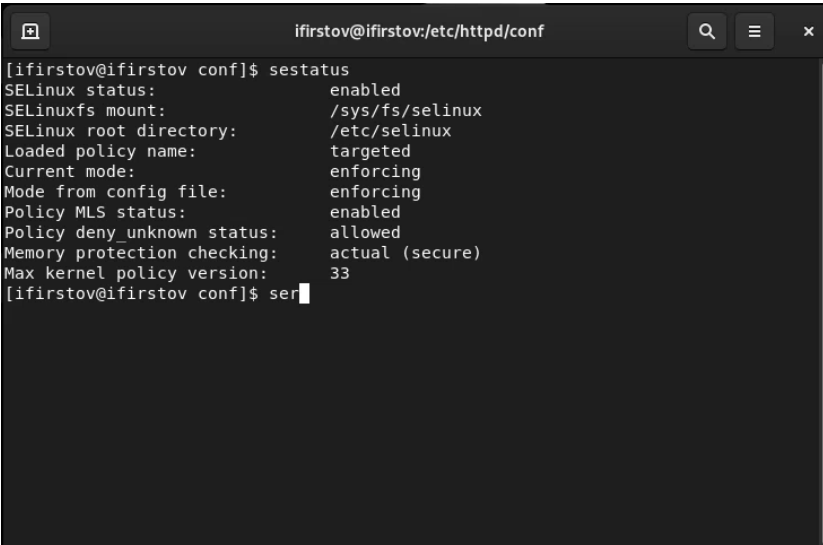
Apache HTTP-сервер (является искажённым сокращением от англ. a patchy server; среди русских пользователей общепринято переводное апа́ч) — свободный веб-сервер.

Apache является кроссплатформенным ПО, поддерживает операционные системы Linux, BSD, macOS, Microsoft Windows, Novell NetWare, BeOS.

Основными достоинствами Apache считаются надёжность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и т. д. Поддерживает IPv4.

# Выполнение лабораторной работы

Проверил режим работы SELinux (рис. [-@fig:001])

A terminal window titled 'ifirstov@ifirstov:/etc/httpd/conf' with search, menu, and close icons in the title bar. The terminal shows the output of the 'sestatus' command. The output lists various SELinux settings: status is enabled, SELinuxfs is mounted at /sys/fs/selinux, the root directory is /etc/selinux, the loaded policy name is targeted, the current mode is enforcing, the mode from the config file is enforcing, the policy MLS status is enabled, the policy deny unknown status is allowed, memory protection checking is actual (secure), and the max kernel policy version is 33. The prompt is '[ifirstov@ifirstov conf]\$' and the next command 'se' is partially entered.

```
[ifirstov@ifirstov conf]$ 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
[ifirstov@ifirstov conf]$ se
```

Рис. 1: SELinux работает в режиме enforcing политики targeted

Проверил работу сервера apache (рис. [-@fig:002])



```
ifirstov@ifirstov:/etc/httpd/conf — /bin/systemctl status httpd.service
Memory protection checking:    actual (secure)
Max kernel policy version:    33
[ifirstov@ifirstov conf]$ 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 pre>
   Active: active (running) since Sat 2022-10-15 21:31:59 MSK; 2min 22s ago
     Docs: man:httpd.service(8)
  Main PID: 40900 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes>
     Tasks: 213 (limit: 12212)
    Memory: 22.6M
       CPU: 81ms
    CGroup: /system.slice/httpd.service
            └─40900 /usr/sbin/httpd -DFOREGROUND
              └─40901 /usr/sbin/httpd -DFOREGROUND
                └─40905 /usr/sbin/httpd -DFOREGROUND
                  └─40906 /usr/sbin/httpd -DFOREGROUND
                    └─40908 /usr/sbin/httpd -DFOREGROUND

окт 15 21:31:59 ifirstov.localdomain systemd[1]: Starting The Apache HTTP Serve>
окт 15 21:31:59 ifirstov.localdomain systemd[1]: Started The Apache HTTP Server>
окт 15 21:31:59 ifirstov.localdomain httpd[40900]: Server configured, listening>
lines 1-19/19 (END)
```

Рис. 2: service httpd status

Проверил состояние переключателей SELinux для Apache(рис. [-@fig:003])

```
ifirstov@ifirstov:/etc/httpd/conf
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
httpd_use_cifs               off
httpd_use_fusefs             off
httpd_use_gpg                off
httpd_use_nfs                off
httpd_use_openscryptoki      off
httpd_use_openstack          off
httpd_use_sasl               off
httpd_verify_dns             off
[ifirstov@ifirstov conf]$
```

Рис. 3: остояние переключателей SELinux

Определите тип файлов и поддиректорий, находящихся в директории /var/www, после чего создал файл test.html (рис. [-@fig:004])

```
ifirstov@ifirstov:/etc/httpd/conf
Auditallowxperm: 0 Dontauditxperm: 0
Ibendportcon: 0 Ibpkeycon: 0
Initial SIDs: 27 Fs_use: 33
Genfscon: 106 Portcon: 651
Netifcon: 0 Nodecon: 0
[ifirstov@ifirstov conf]$ ls -lZ /var/www
ls: невозможно получить доступ к '/var/www': Нет такого файла или каталога
[ifirstov@ifirstov conf]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 15
:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 16 15
:10 html
[ifirstov@ifirstov conf]$ ls -lZ /var/www/html/
итого 0
[ifirstov@ifirstov conf]$ ls -l /var/www/html/
итого 0
[ifirstov@ifirstov conf]$ ls -l /var/www/
итого 0
drwxr-xr-x. 2 root root 6 мая 16 15:10 cgi-bin
drwxr-xr-x. 2 root root 6 мая 16 15:10 html
[ifirstov@ifirstov conf]$ sudo touch /var/www/html/test.html
[ifirstov@ifirstov conf]$ sudo nano /var/www/html/test.html
[ifirstov@ifirstov conf]$
```

Рис. 4: Тип файлов в директории /var/www

Зашел через браузер и проверил отображение файла test.html.(рис. [-@fig:005])

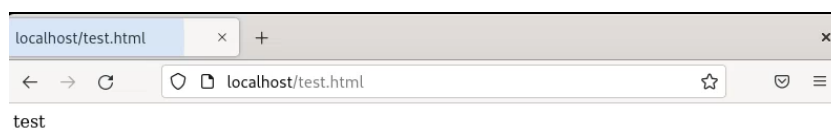


Рис. 5: Отображение файла test.html

Изменил контекст test.html.(рис. [-@fig:006])

```
ifirstov@ifirstov:/etc/httpd/conf
итого 0
[ifirstov@ifirstov conf]$ ls -l /var/www/html/
итого 0
[ifirstov@ifirstov conf]$ ls -l /var/www/
итого 0
drwxr-xr-x. 2 root root 6 мая 16 15:10 cgi-bin
drwxr-xr-x. 2 root root 6 мая 16 15:10 html
[ifirstov@ifirstov conf]$ sudo touch /var/www/html/test.html
[ifirstov@ifirstov conf]$ sudo nano /var/www/html/test.html
[ifirstov@ifirstov conf]$ ls -l /var/www/html/
итого 4
-rw-r--r--. 1 root root 36 окт 15 21:37 test.html
[ifirstov@ifirstov conf]$ chcon -t samba_share_t /var/www/html/test.html
chcon: не удалось изменить контекст безопасности '/var/www/html/test.html' на «unconfined_u:object_r:samba_share_t:s0»: Операция не позволена
[ifirstov@ifirstov conf]$ sudo chcon -t samba_share_t /var/www/html/test.html
[ifirstov@ifirstov conf]$ ls -l /var/www/html/
итого 4
-rw-r--r--. 1 root root 36 окт 15 21:37 test.html
[ifirstov@ifirstov conf]$ ls -lZ /var/www/html/
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 36 окт 15 21:37 test.html
[ifirstov@ifirstov conf]$
```

Рис. 6: Контекст test.html

Зашел через браузер и снова проверил отображение файла test.html. Из-за изменения контекста произошла ошибка доступа(рис. [-@fig:007])

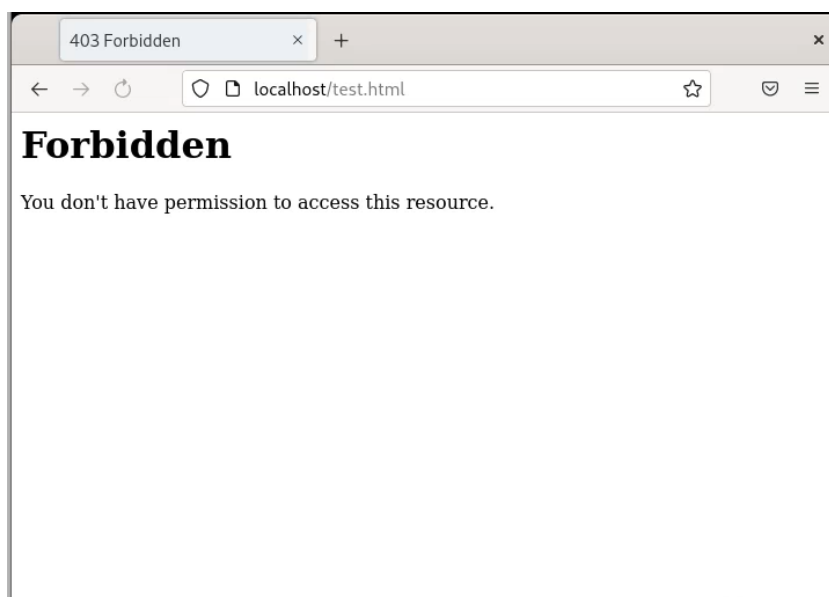


Рис. 7: Ошибка доступа

В логах также отображается ошибка доступа(рис. [-@fig:007])

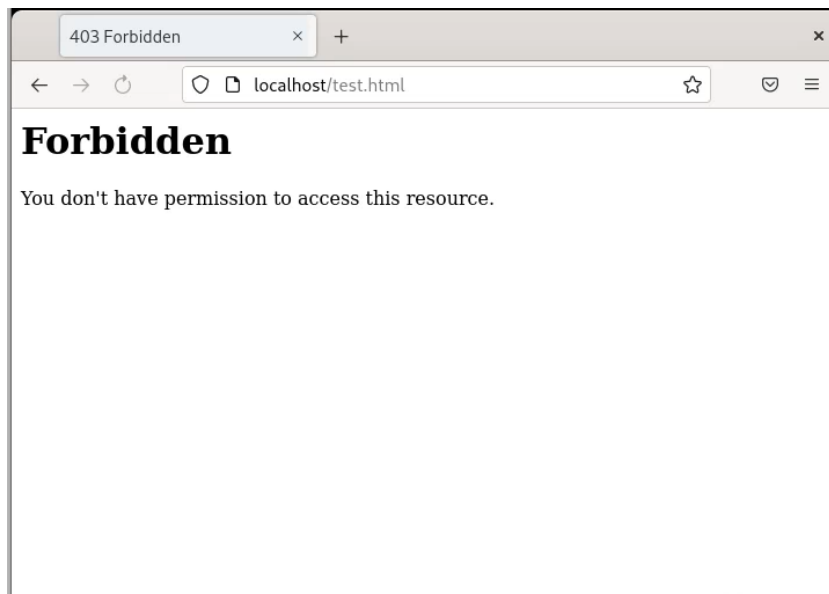


Рис. 8: Просмотр логов

# Выводы

Я развил навыки администрирования ОС Linux

# Список литературы

[https://ru.wikipedia.org/wiki/Apache\\_HTTP\\_Server](https://ru.wikipedia.org/wiki/Apache_HTTP_Server)