

# Лабораторная работа №6

Мандатное разграничение прав в Linux

---

Рыбалко Элина<sup>1</sup>

2022, 13 October, 2022 Moscow, Russian Federation

<sup>1</sup>RUDN University, Moscow, Russian Federation

- Приобретение практических навыков работы мандатным разграничением прав на операционной системы Linux.

## Цель выполнения лабораторной работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux<sup>1</sup>. Проверить работу SELinx на практике совместно с веб-сервером Apache.

- Подготовка лабораторного стенда.
- Работа с SELinux.

```
[eprybalko@eprybalko ~]$ getenforce
Enforcing
[eprybalko@eprybalko ~]$ 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
[eprybalko@eprybalko ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
Unit httpd.service could not be found.
```

Рис. 1: Подготовка лабораторного стенда

# Результаты выполнения лабораторной работы

```
[eprybalko@eprybalko ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor prese
t: disabled)
   Active: inactive (dead)
     Docs: man:httpd(8)
          man:apachectl(8)
[eprybalko@eprybalko ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[eprybalko@eprybalko ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
Failed to start httpd.service: Access denied
See system logs and 'systemctl status httpd.service' for details.
[eprybalko@eprybalko ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor prese
t: disabled)
   Active: active (running) since Чт 2022-10-13 15:15:04 MSK; 7s ago
     Docs: man:httpd(8)
          man:apachectl(8)
  Main PID: 3431 (httpd)
    Status: "Processing requests..."
```

Рис. 2: Подготовка лабораторного стенда

# Результаты выполнения лабораторной работы

```
[eprybalko@eprybalko ~]$ seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes:          130      Permissions:      272
Sensitivities:    1        Categories:      1024
Types:            4793     Attributes:       253
Users:            8        Roles:           14
Booleans:         316     Cond. Expr.:     362
Allow:            107834   Neverallow:      0
Auditallow:       158     Dontaudit:       10022
Type_trans:       18153   Type_change:     74
Type_member:      35      Role_allow:      37
Role_trans:       414     Range_trans:     5899
Constraints:      143     Validatetrans:   0
Initial SIDs:     27      Fs_use:          32
Genfscon:         103     Portcon:         614
Netifcon:         0       Nodecon:         0
Permissives:      0       Polcap:          5

[eprybalko@eprybalko ~]$ 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
[eprybalko@eprybalko ~]$ ls -lZ /var/www/html
[eprybalko@eprybalko ~]$ su
Пароль:
[root@eprybalko eprybalko]# vim /var/www/html/test.html
[root@eprybalko eprybalko]# ls -lZ /var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@eprybalko eprybalko]# chcon -t samba_share_t /var/www/html/test.html
[root@eprybalko eprybalko]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined u:object r:samba share t:s0 /var/www/html/test.
```

Рис. 3: Просмотр статистики и типов файлов

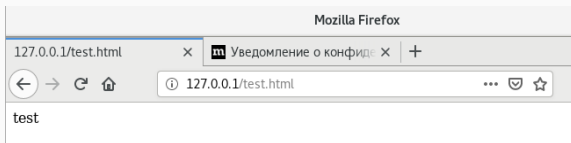


Рис. 4: Промотр файла через браузер разрешён



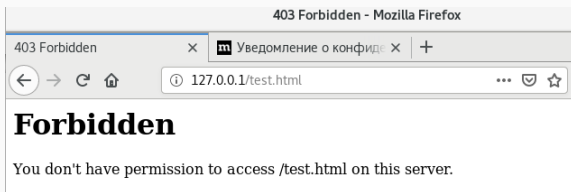
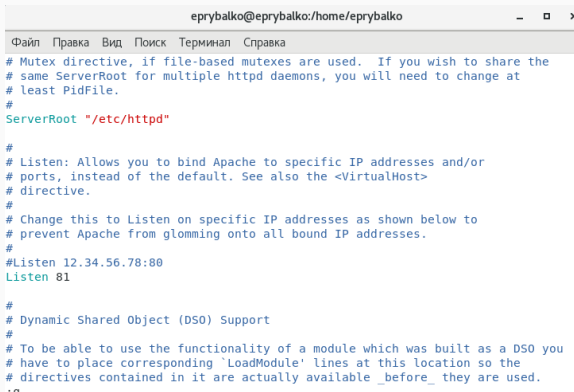


Рис. 5: Просмотр файла через браузер запрещён

# Результаты выполнения лабораторной работы



```
eprybalko@eprybalko:/home/eprybalko
Файл Правка Вид Поиск Терминал Справка
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# 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.
#
```

Рис. 6: Изменение файла и номера порта

```
[root@eprybalko eprybalko]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@eprybalko eprybalko]# 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@eprybalko eprybalko]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@eprybalko eprybalko]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@eprybalko eprybalko]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@eprybalko eprybalko]# service httpd start
Redirecting to /bin/systemctl start httpd.service
```

Рис. 7: Добавление 81 порта

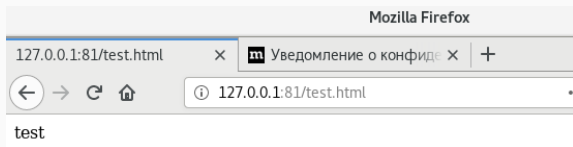


Рис. 8: Просмотр файла через 81 порт

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinux на практике совместно с веб-сервером Apache.