

# **Лабораторная работа №6**

**Мандатное разграничение прав в Linux.**

Крутова Екатерина Дмитриевна

# Содержание

|                                       |           |
|---------------------------------------|-----------|
| <b>Цель работы</b>                    | <b>5</b>  |
| <b>Выполнение лабораторной работы</b> | <b>6</b>  |
| <b>Выводы</b>                         | <b>12</b> |

## Список иллюстраций

|    |   |    |
|----|---|----|
| 1  | Проверка работы SELinux . . . . .   | 6  |
| 2  | Проверка работы веб-сервера . . . . .                                       | 6  |
| 3  | Просмотра контекста безопасности . . . . .                                  | 7  |
| 4  | Просмотр текущего состояния переключателей SELinux . . . . .                | 7  |
| 5  | Просмотр статистики по политике . . . . .                                   | 7  |
| 6  | тип файлов и поддиректорий, находящихся в директории /var/www . . .         | 8  |
| 7  | тип файлов, находящихся в директории /var/www/html . . . . .                | 8  |
| 8  | /var/www/html/test.html . . . . .   | 8  |
| 9  | Контекст файла . . . . .  | 8  |
| 10 | Веб-сервер . . . . .  | 8  |
| 11 | Проверка контекста файла . . . . .  | 9  |
| 12 | Изменение контекста файла . . . . .   | 9  |
| 13 | Ошибка доступа к веб-серверу . . . . .                                      | 9  |
| 14 | Просмотр log-файлов веб-сервера Apache . . . . .                            | 9  |
| 15 | Изменение /etc/httpd/httpd.conf . . . . .                                   | 10 |
| 16 | Перезапуск веб-сервера Apache . . . . .                                     | 10 |
| 17 | Просмотр файла /var/log/http/error_log . . . . .                            | 10 |
| 18 | Возвращение контекста httpd_sys_content__t к файлу /var/www/html/ test.html | 10 |
| 19 | Перезапуск веб-сервера Apache . . . . .                                     | 11 |
| 20 | Веб-сервер Apache . . . . .   | 11 |
| 21 | Исправление конфигурационного файла apache . . . . .                        | 11 |
| 22 | Удаление привязки http_port_t к 81 порту . . . . .                          | 11 |
| 23 | Удаление файла /var/www/html/test.html . . . . .                            | 11 |

## **Список таблиц**

## **Цель работы**

Целью данной работы является развитие навыков администрирования ОС Linux, получение первого практического знакомства с технологией SELinux. Проверка работы SELinux на практике совместно с веб-сервером Apache.

# Выполнение лабораторной работы

1. Создание программы (рис. [-@fig:001] - [-@fig:023]).

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

Рис. 1: Проверка работы SELinux

```
[edkrutova@edkrutova ~]$ 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; preset: disabled)
   Active: active (running) since Sat 2024-10-12 09:45:31 MSK; 4min 6s ago
     Docs: man:httpd.service(8)
   Main PID: 3966 (httpd)
   Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/se
   Tasks: 177 (limit: 12196)
   Memory: 9.4M
     CPU: 401ms
   CGroup: /system.slice/httpd.service
           └─3966 /usr/sbin/httpd -DFOREGROUND
             └─3974 /usr/sbin/httpd -DFOREGROUND
               └─3978 /usr/sbin/httpd -DFOREGROUND
                 └─3979 /usr/sbin/httpd -DFOREGROUND
                   └─3980 /usr/sbin/httpd -DFOREGROUND

Oct 12 09:45:30 edkrutova systemd[1]: Starting The Apache HTTP Server...
Oct 12 09:45:31 edkrutova httpd[3966]: AH00558: httpd: Could not reliably determine the s
Oct 12 09:45:31 edkrutova systemd[1]: Started The Apache HTTP Server.
Oct 12 09:45:31 edkrutova httpd[3966]: Server configured, listening on: port 80
lines 1-20/20 (END)
```

Рис. 2: Проверка работы веб-сервера

```
[edkrutova@edkrutova ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 3966 0.0 0.4 20364 8384 ? Ss 09:45
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3974 0.0 0.2 22096 5584 ? S 09:45
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3978 0.0 0.2 1112656 6024 ? Sl 09:45
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3979 0.0 0.2 981520 6028 ? Sl 09:45
0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3980 0.0 0.2 981520 5980 ? Sl 09:45
0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 edkruto+ 4677 0.0 0.1 221796 2432 pt
s/1 S+ 09:50 0:00 grep --color=auto httpd
[edkrutova@edkrutova ~]$
```

Рис. 3: Просмотра контекста безопасности

```
[edkrutova@edkrutova ~]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

-v Verbose check of process and file contexts.
-b Display current state of booleans.

Without options, show SELinux status.
[edkrutova@edkrutova ~]$
```

Рис. 4: Просмотр текущего состояния переключателей SELinux

```
[edkrutova@edkrutova ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version: 33 (MLS enabled)
Target Policy: selinux
Handle unknown classes: allow
Classes: 135 Permissions: 457
Sensitivities: 1 Categories: 1024
Types: 5145 Attributes: 259
Users: 8 Roles: 15
Booleans: 356 Cond. Expr.: 388
Allow: 65500 Neverallow: 0
Auditallow: 176 Dontaudit: 8682
Type_trans: 271770 Type_change: 94
Type_member: 37 Range_trans: 5931
Role allow: 40 Role_trans: 417
Constraints: 70 Validatetrans: 0
MLS Constrain: 72 MLS Val. Tran: 0
Permissives: 4 Polcap: 6
Defaults: 7 Typebounds: 0
Allowxperm: 0 Neverallowxperm: 0
Auditallowxperm: 0 Dontauditxperm: 0
Ibendportcon: 0 Ibpkeycon: 0
Initial SIDs: 27 Fs_use: 35
Genfscon: 109 Portcon: 665
Netifcon: 0 Nodecon: 0
[edkrutova@edkrutova ~]$
```

Рис. 5: Просмотр статистики по политике

```

[edkrutova@edkrutova ~]$ ls -lZ /var/www/
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Aug 8 19:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Aug 8 19:30 html
[edkrutova@edkrutova ~]$

```

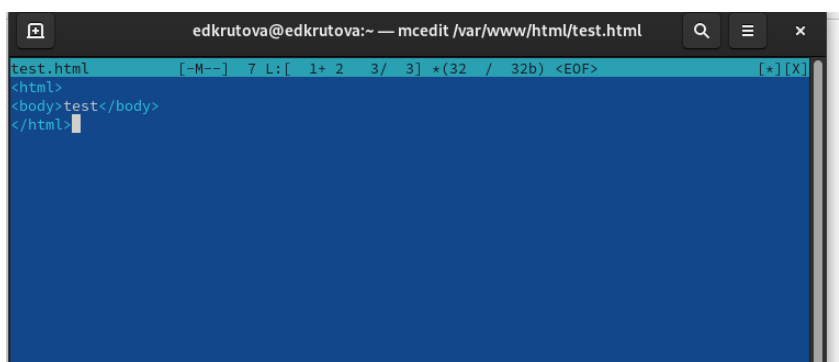
Рис. 6: тип файлов и поддиректорий, находящихся в директории /var/www

```

[edkrutova@edkrutova ~]$ ls -lZ /var/www/html/
total 0
[edkrutova@edkrutova ~]$

```

Рис. 7: тип файлов, находящихся в директории /var/www/html



```

test.html  [-M--]  7 L: [ 1+ 2  3/  3] *(32 / 32b) <EOF>  [*] [X]
<html>
<body>test</body>
</html>

```

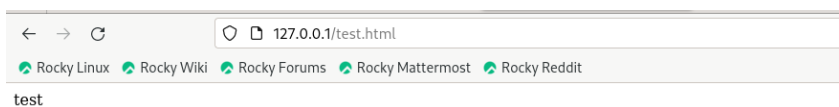
Рис. 8: /var/www/html/test.html

```

[edkrutova@edkrutova ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[edkrutova@edkrutova ~]$

```

Рис. 9: Контекст файла



```

test

```

Рис. 10: Веб-сервер



```
[edkrutova@edkrutova ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[edkrutova@edkrutova ~]$
```

Рис. 11: Проверка контекста файла

```
[edkrutova@edkrutova ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] password for edkrutova:
[edkrutova@edkrutova ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[edkrutova@edkrutova ~]$
```

Рис. 12: Изменение контекста файла

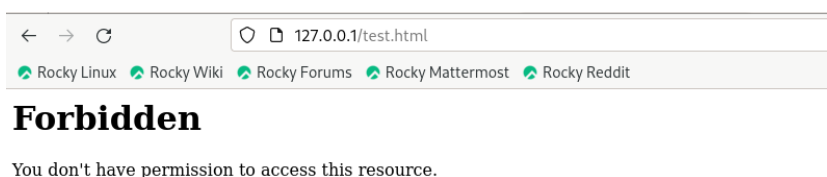


Рис. 13: Ошибка доступа к веб-серверу

```
[root@edkrutova ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 32 Oct 12 10:00 /var/www/html/test.html
[root@edkrutova ~]# tail /var/log/messages
Oct 12 10:06:51 edkrutova setroubleshoot[5331]: SELinux is preventing /usr/sbin/httpd from
getattr access on the file /var/www/html/test.html. For complete SELinux messages run: seatt
ert -l 5d9e1de3-816a-403e-a79a-c56b17a3524c
Oct 12 10:06:51 edkrutova setroubleshoot[5331]: SELinux is preventing /usr/sbin/httpd from
getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 c
onfidence) suggests *****#012#012If you want to fix the label. #012/va
r/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run resto
recon. The access attempt may have been stopped due to insufficient permissions to access a
parent directory in which case try to change the following command accordingly.#012Do#012#
/sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 conf
idence) suggests *****#012#012If you want to treat test.html as public con
tent#012Then you need to change the label on test.html to public_content_t or public_conte
nt_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) sug
gests *****#012#012If you believe that httpd should be allowed getat
tr access on the test.html file by default.#012Then you should report this as a bug.#012You
can generate a local policy module to allow this access.#012Do#012allow this access for no
w by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 3
00 -i my-httpd.pp#012
```

Рис. 14: Просмотр log-файлов веб-сервера Apache

```
httpd.conf [-M--] 9 L: [ 1+ 1 2/ 2] *(28 / 28b) <EOF> [*] [X]
ServerName test.ru
Listen 81
```

Рис. 15: Изменение /etc/httpd/httpd.conf

```
[root@edkrutova ~]# systemctl restart httpd
[root@edkrutova ~]#
```

Рис. 16: Перезапуск веб-сервера Apache

```
[root@edkrutova ~]# cat /var/log/httpd/error_log
[Sat Oct 12 09:45:31.034713 2024] [core:notice] [pid 3966:tid 3966] SELinux policy enabled;
httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 12 09:45:31.052507 2024] [suexec:notice] [pid 3966:tid 3966] AH01232: suEXEC mecha
nism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, usin
g fe80::a00:27ff:feaa:a7a7%enp0s3. Set the 'ServerName' directive globally to suppress this
message
[Sat Oct 12 09:45:31.135375 2024] [lbmethod_heartbeat:notice] [pid 3966:tid 3966] AH02282:
No slotmem from mod_heartbeat
[Sat Oct 12 09:45:31.159702 2024] [mpm_event:notice] [pid 3966:tid 3966] AH00489: Apache/2.
4.57 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 12 09:45:31.159745 2024] [core:notice] [pid 3966:tid 3966] AH00094: Command line:
'/usr/sbin/httpd -D FOREGROUND'
[Sat Oct 12 10:06:24.482358 2024] [core:error] [pid 3980:tid 4115] (13)Permission denied: [
client 127.0.0.1:52852] AH00035: access to /test.html denied (filesystem path '/var/www/htm
l/test.html') because search permissions are missing on a component of the path
[Sat Oct 12 10:06:48.756499 2024] [core:error] [pid 3980:tid 4118] (13)Permission denied: [
client 127.0.0.1:33166] AH00035: access to /test.html denied (filesystem path '/var/www/htm
l/test.html') because search permissions are missing on a component of the path
[Sat Oct 12 10:13:32.248089 2024] [mpm_event:notice] [pid 3966:tid 3966] AH00492: caught SI
GWINCH, shutting down gracefully
[Sat Oct 12 10:13:33.414158 2024] [core:notice] [pid 5481:tid 5481] SELinux policy enabled;
httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 12 10:13:33.417423 2024] [suexec:notice] [pid 5481:tid 5481] AH01232: suEXEC mecha
nism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, usin
g fe80::a00:27ff:feaa:a7a7%enp0s3. Set the 'ServerName' directive globally to suppress this
message
[Sat Oct 12 10:13:33.455860 2024] [lbmethod_heartbeat:notice] [pid 5481:tid 5481] AH02282:
No slotmem from mod_heartbeat
[Sat Oct 12 10:13:33.473403 2024] [mpm_event:notice] [pid 5481:tid 5481] AH00489: Apache/2.
4.57 (Rocky Linux) configured -- resuming normal operations
[Sat Oct 12 10:13:33.473451 2024] [core:notice] [pid 5481:tid 5481] AH00094: Command line:
'/usr/sbin/httpd -D FOREGROUND'
[root@edkrutova ~]#
```

Рис. 17: Просмотр файла /var/log/http/error\_log

```
[root@edkrutova ~]# semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[root@edkrutova ~]# semanage port -l | grep http_port_t
http_port_t tcp 81, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t tcp 5988
[root@edkrutova ~]#
```

Рис. 18: Возвращение контекста httpd\_sys\_content\_\_t к файлу /var/www/html/ test.html

```
[root@edkrutova ~]# systemctl restart httpd
[root@edkrutova ~]#
```

Рис. 19: Перезапуск веб-сервера Apache

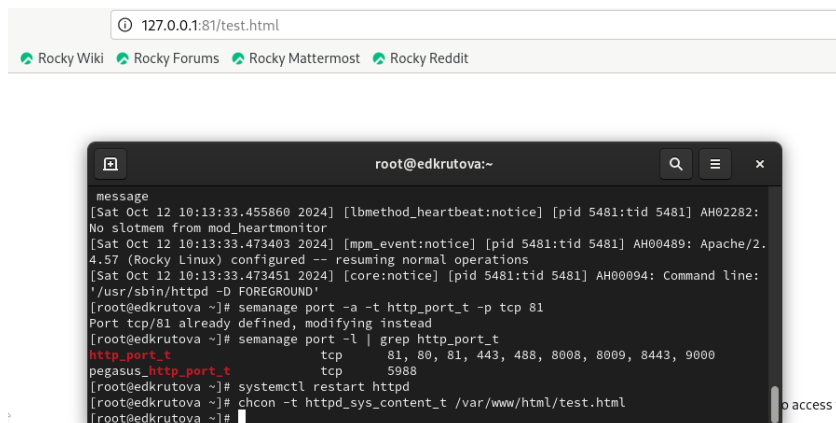


Рис. 20: Веб-сервер Apache

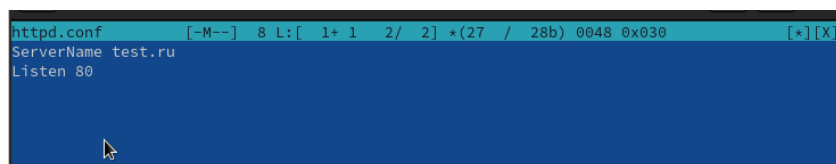


Рис. 21: Исправление конфигурационного файла apache

```
[root@edkrutova ~]# semanage port -d -t http_port_t -p tcp 81
[root@edkrutova ~]# 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@edkrutova ~]#
```

Рис. 22: Удаление привязки http\_port\_t к 81 порту

```
[root@edkrutova ~]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@edkrutova ~]#
```

Рис. 23: Удаление файла /var/www/html/test.html

## **Выводы**

Я развила навыки администрирования ОС Linux, получила первое практическое знакомство с технологией SELinux. Проверила работу SELinux на практике совместно с веб-сервером Apache.