

Лабораторная работа № 5.

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов.

Машков И. Е.

08 марта 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Машков Илья Евгеньевич
- Студент 2-го курс, группа НКАбд-03-23
- Российский университет дружбы народов
- 1132231984@pfur.ru
- <https://github.com/7S7eVe7N7>

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

```
[iemashkov@localhost ~]$ getenforce
Enforcing
[iemashkov@localhost ~]$ 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
[iemashkov@localhost ~]$
```

Рис. 1: проверка режима работы SELinux

```
[iemashkov@localhost ~]$ sudo systemctl start httpd
[iemashkov@localhost ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[iemashkov@localhost ~]$ 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 prese
   Active: active (running) since Sat 2025-05-03 17:33:44 MSK; 52s ago
     Docs: man:httpd.service(8)
  Main PID: 129016 (httpd)
    Status: "Running, listening on: port 80"
     Tasks: 213 (limit: 37628)
    Memory: 41.9M
    CGroup: /system.slice/httpd.service
            └─129016 /usr/sbin/httpd -DFOREGROUND
              └─129023 /usr/sbin/httpd -DFOREGROUND
                └─129024 /usr/sbin/httpd -DFOREGROUND
                  └─129025 /usr/sbin/httpd -DFOREGROUND
                    └─129026 /usr/sbin/httpd -DFOREGROUND
```

Рис. 2: Проверка работы Apache

```
[iemashkov@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0  root      129016  0.0  0.1 258208 10996 ?
Ss  17:33  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  129023  0.0  0.1 262912  8464 ?
S   17:33  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  129024  0.0  0.3 2697028 18260 ?
Sl  17:33  0:01 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  129025  0.1  0.3 2500364 18344 ?
Sl  17:33  0:01 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0  apache  129026  0.1  0.3 2500364 18332 ?
Sl  17:33  0:01 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 iemashk+ 129600 0.0  0.0 2
22012 1096 pts/0 S+ 17:54  0:00 grep --color=auto httpd
[iemashkov@localhost ~]$
```

Рис. 3: Контекст безопасности Apache

Выполнение лабораторной работы

```
[iemand@localhost ~]$ sestatus -b httpd
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

Policy booleans:
abrt_anon_write                off
abrt_handle_event              off
abrt_upload_watch_anon_write   on
antivirus_can_scan_system      off
antivirus_use_jit              off
auditadm_exec_content          on
authlogin_nsswitch_use_ldap     off
authlogin_radius               off
authlogin_yubikey              off
awstats_purge_apache_log_files off
boinc_execmem                  on
```


Выполнение лабораторной работы

```
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          31 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:                  132    Permissions:              464
Sensitivities:            1      Categories:              1024
Types:                    5015   Attributes:              258
Users:                    8       Roles:                   15
Booleans:                 349    Cond. Expr.:            399
Allow:                    116272  Neverallow:              0
Auditallow:               172    Dontaudit:              10529
Type_trans:               262670  Type_change:             94
Type_member:              37      Range_trans:            5989
Role_allow:               40      Role_trans:             421
Constraints:              72      Validatetrans:          0
MLS Constrains:           72      MLS Val. Tran:          0
Permissives:              0       Polcap:                 5
Defaults:                 7       Typebounds:             0
Allowxperm:               0       Neverallowxperm:        0
Auditallowxperm:          0       Dontauditxperm:         0
Ibendportcon:             0       Ibkeycon:               0
Initial SIDs:             27      Fs_use:                 34
Genfscon:                 107     Portcon:                649
```

```
[iemashkov@localhost ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 фев 19 23
:08 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 фев 19 23
:08 html
```

Рис. 6: Типы поддиректорий

```
[iemashkov@localhost ~]$ ls -lZ /var/www/html  
итого 0
```

Рис. 7: Типы файлов

html

<html>

<body>test</body>

</html>

```
[iemashkov@localhost ~]$ sudo touch /var/www/html/test.html
[sudo] пароль для iemashkov:
[iemashkov@localhost ~]$ sudo nano /var/www/html/test.html
[iemashkov@localhost ~]$ sudo cat /var/www/html/test.html
<html>
<body>test</body>
</html>
```

Рис. 8: Создание файла

```
[iemashkov@localhost ~]$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 мая  3 1
7:59 test.html
```

Рис. 9: Контекст файла

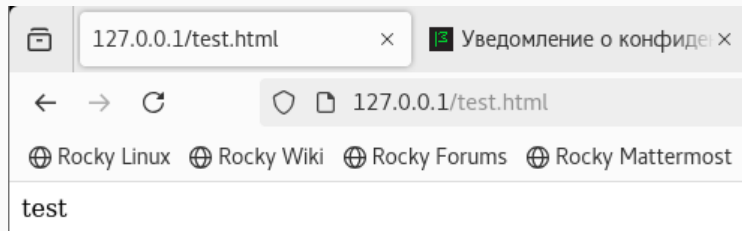
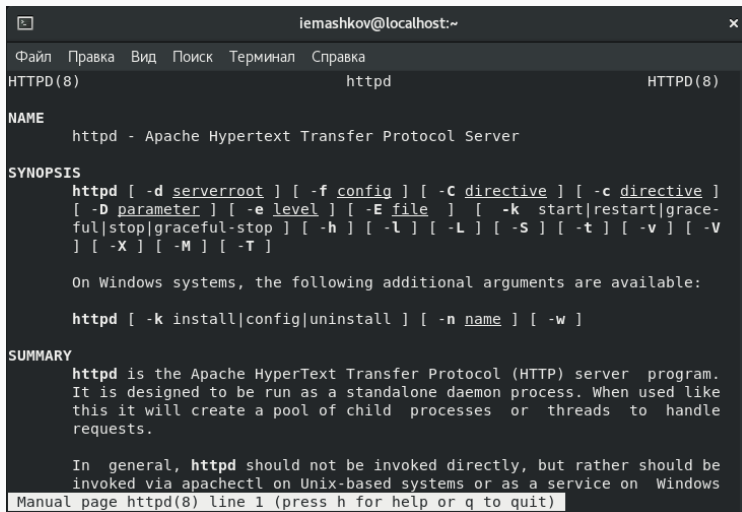


Рис. 10: Отображение файла



```
iemashkov@localhost:~
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|graceful-stop ] [ -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
    Manual page httpd(8) line 1 (press h for help or q to quit)
```

```
[iemashkov@localhost ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] пароль для iemashkov:
[iemashkov@localhost ~]$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 мая  3 17:59 test.html
[iemashkov@localhost ~]$
```

Рис. 12: Изменение контекста

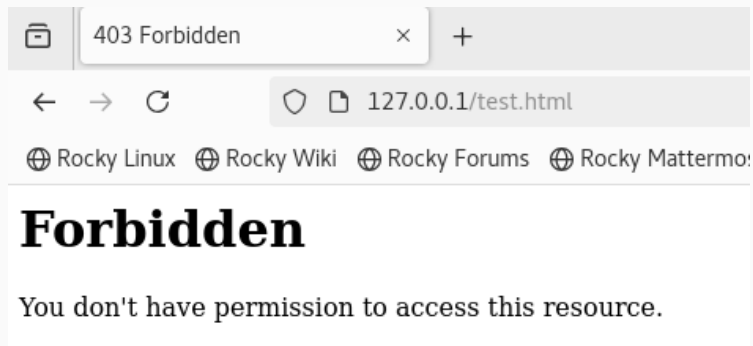


Рис. 13: Отображение файла

```
[iemashkov@localhost ~]$ ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 мая  3 17:59 /var/www/html/test.html
[iemashkov@localhost ~]$ sudo tail /var/log/messages
May  3 18:06:12 localhost systemd[1]: timedatex.service: Succeeded.
May  3 18:06:13 localhost dbus-daemon[826]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
May  3 18:06:13 localhost systemd[1]: Started SETroubleshoot daemon for processing new SELinux denial logs.
May  3 18:06:14 localhost setroubleshoot[131479]: failed to retrieve rpm info for /var/www/html/test.html
May  3 18:06:14 localhost dbus-daemon[826]: [system] Activating service name='org.fedoraproject.SetroubleshootPrivileged' requested by ':1.1093' (uid=984 pid=131479 comm="/usr/libexec/platform-python -Es /usr/sbin/setroub" label="system_u:s
```

Рис. 14: Попытка прочесть лог-файл

```
# 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
#
```

Рис. 15: Изменение порта

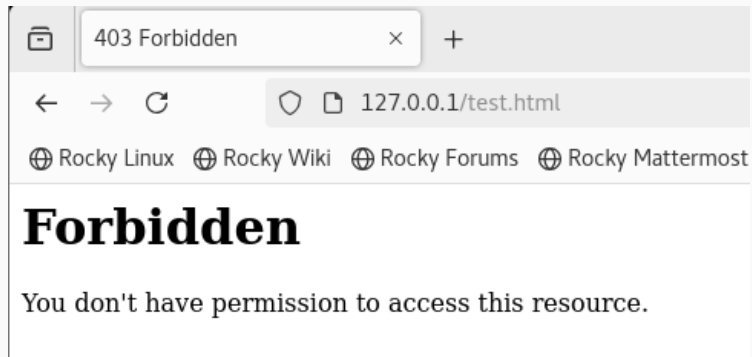


Рис. 16: Попытка прослушивания другого порта

```
[iemashkov@localhost ~]$ sudo tail -n1 /var/log/messages  
May  3 18:12:19 localhost org.gnome.Shell.desktop[2063]: libinput error: event2  
- AT Translated Set 2 keyboard: client bug: event processing lagging behind by  
12ms, your system is too slow
```

Рис. 17: Проверка лог-файлов

```
[iemashkov@localhost ~]$ sudo cat /var/log/httpd/error_log
[Sat May 03 17:33:44.062054 2025] [core:notice] [pid 129016:tid 140193110817088]
  SELinux policy enabled; httpd running as context system_u:system_r:httpd t:s0
[Sat May 03 17:33:44.065107 2025] [suexec:notice] [pid 129016:tid 14019311081708
8] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain
name, using localhost.localdomain. Set the 'ServerName' directive globally to s
uppress this message
[Sat May 03 17:33:44.081069 2025] [lbmethod_heartbeat:notice] [pid 129016:tid 14
0193110817088] AH02282: No slotmem from mod_heartbeat
[Sat May 03 17:33:44.082015 2025] [http2:warn] [pid 129016:tid 140193110817088]
AH02951: mod_ssl does not seem to be enabled
[Sat May 03 17:33:44.085125 2025] [mpm_event:notice] [pid 129016:tid 14019311081
7088] AH00489: Apache/2.4.37 (Rocky Linux) configured -- resuming normal operati
ons
[Sat May 03 17:33:44.085152 2025] [core:notice] [pid 129016:tid 140193110817088]
  AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Sat May 03 18:02:18.518130 2025] [autoindex:error] [pid 129025:tid 140192514164
480] [client 127.0.0.1:37444] AH01276: Cannot serve directory /var/www/html/: No
  matching DirectoryIndex (index.html) found, and server-generated directory inde
x forbidden by Options directive
[Sat May 03 18:05:46.981411 2025] [core:error] [pid 129025:tid 140192396588800]
(13)Permission denied: [client 127.0.0.1:46728] AH00035: access to /test.html de
```

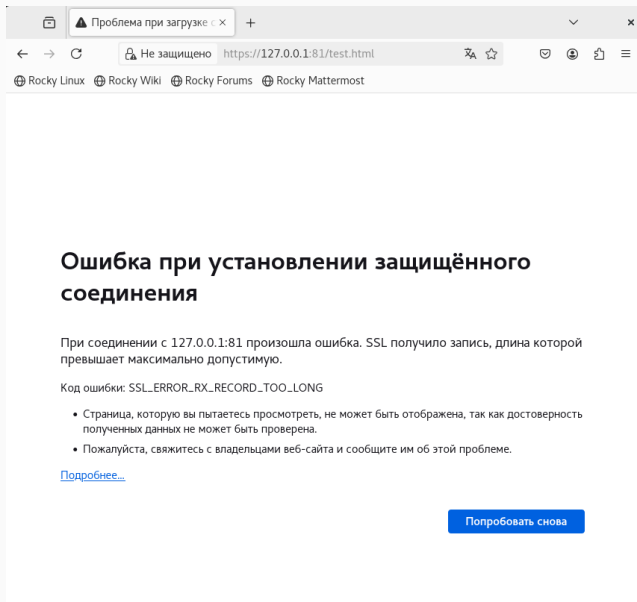
Рис. 18: Проверка лог-файлов

```
[iemashkov@localhost ~]$ semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
               {import,export,login,user,port,ibpkey,ibendport,interface,module
               ,node,fcontext,boolean,permissive,dontaudit}
               ...
semanage: error: unrecognized arguments: -p 81
[iemashkov@localhost ~]$ semanage port -l | grep http_port_t
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[iemashkov@localhost ~]$ sudo 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
[iemashkov@localhost ~]$
```

Рис. 19: Проверка портов

```
[iemashkov@localhost ~]$ sudo systemctl restart httpd  
[iemashkov@localhost ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html  
[iemashkov@localhost ~]$ sudo systemctl restart httpd  
[iemashkov@localhost ~]$
```

Рис. 20: Перезапуск сервера



```
[iemashkov@localhost ~]$ sudo nano /etc/httpd/conf/httpd.conf  
[iemashkov@localhost ~]$ sudo semanage port -d -t http_port_t -p tcp 81  
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
```

Рис. 22: Проверка порта 81

```
[iemashkov@localhost html]$ ls -lZ /var/www/html  
итого 0  
[iemashkov@localhost html]$
```

Рис. 23: Удаление файла

В ходе выполнения данной лабораторной работы были развиты навыки администрирования ОС Linux, получено первое практическое знакомство с технологией SELinux и проверена работа SELinux на практике совместно с веб-сервером Apache.