

# **Лабораторная работа №6**

**Основы Информационной Безопасности**

Чистов Даниил Максимович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
<b>3</b>	<b>Выводы</b>	<b>13</b>
<b>4</b>	<b>Список литературы</b>	<b>14</b>

# Список иллюстраций

2.1	Вывод команды <code>service httpd status</code> . . . . .	5
2.2	Процессы Apache . . . . .	6
2.3	Состояние переключателей SELinux для Apache . . . . .	6
2.4	Статистика по политике . . . . .	7
2.5	Типы файлов в <code>/var/www</code> . . . . .	7
2.6	Данные по <code>/var/www/html</code> . . . . .	7
2.7	<code>test.html</code> . . . . .	8
2.8	<code>test.html</code> - контекст . . . . .	8
2.9	<code>test.html</code> - в браузере . . . . .	8
2.10	<code>test.html</code> - контекст . . . . .	9
2.11	<code>test.html</code> - новый контекст . . . . .	9
2.12	<code>test.html</code> - отказано в доступе . . . . .	9
2.13	<code>test.html</code> - расследование причины отказа . . . . .	10
2.14	Веб-сервер на прослушивании порта 81 . . . . .	10
2.15	Веб-сервер не загружает страничку . . . . .	10
2.16	Расследую ситуацию - прослушивание на порте 81 . . . . .	11
2.17	Расследую ситуацию - отсутствие прав . . . . .	11
2.18	Новый порт - 81 . . . . .	11
2.19	Сайт открывается на порте 81 . . . . .	12
2.20	Завершение работы . . . . .	12

# 1 Цель работы

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

## 2 Выполнение лабораторной работы

Вхожу в систему, убеждаюсь командой `sestatus`, что SELinux работает в режиме enforcing политики targeted (рис. ??).

```
[dmchistov@dmchistov 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
[dmchistov@dmchistov conf]$ getenforce
Enforcing
[dmchistov@dmchistov conf]$
```

Командой `service httpd status` убеждаюсь, что веб-сервер Apache работает (рис. 2.1).

```
[dmchistov@dmchistov 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 preset: disabled)
   Active: active (running) since Fri 2025-05-02 18:17:36 MSK; 10min ago
     Docs: man:httpd.service(8)
  Main PID: 42419 (httpd)
    Status: "Running, listening on: port 80"
   Tasks: 213 (limit: 12238)
  Memory: 33.4M
    CGroup: /system.slice/httpd.service
            └─42419 /usr/sbin/httpd -DFOREGROUND
              └─42428 /usr/sbin/httpd -DFOREGROUND
                └─42429 /usr/sbin/httpd -DFOREGROUND
                  └─42430 /usr/sbin/httpd -DFOREGROUND
                    └─42431 /usr/sbin/httpd -DFOREGROUND

May 02 18:17:36 dmchistov.localdomain systemd[1]: Starting The Apache HTTP Server...
May 02 18:17:36 dmchistov.localdomain systemd[1]: Started The Apache HTTP Server.
May 02 18:17:36 dmchistov.localdomain httpd[42419]: Server configured, listening on: port 80
[dmchistov@dmchistov conf]$
```

Рис. 2.1: Вывод команды `service httpd status`

Командой `ps auxZ | grep httpd` нахожу процессы веб-сервера Apache и определяю

его контекст безопасности - httpd\_t (рис. 2.2).

```
[dmchistov@dmchistov conf]$ ps aux | grep httpd
system_u:system_r:httpd_t:s0 root      42419  0.0  0.5 258204 11088 ?        Ss   18:17   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  42428  0.0  0.4 262908  8288 ?        S    18:17   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  42429  0.0  0.9 2762564 20108 ?      Sl   18:17   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  42430  0.0  0.5 2565900 11936 ?      Sl   18:17   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  42431  0.0  0.6 2500364 13976 ?      Sl   18:17   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0-c1023 dmchist+ 42967  0.0  0.0 222012 1184 pts/0  S+   18:28   0:00 grep --color=auto httpd
```

Рис. 2.2: Процессы Apache

Командой `sestatus -b | grep httpd` смотрю текущее состояние переключателей SELinux для Apache, действительно большинство из них в положении “off” (рис. 2.3).

```
[dmchistov@dmchistov conf]$ sestatus -b | grep httpd
httpd_anon_write off
httpd_builtin_scripting on
httpd_can_check_spam off
httpd_can_connect_ftp off
httpd_can_connect_ldap off
httpd_can_connect_mythtv off
httpd_can_connect_zabbix off
httpd_can_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_redis off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sss off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_enable_openssl off
```

Рис. 2.3: Состояние переключателей SELinux для Apache

Командой `seinfo` смотрю статистику по политике - вижу, что типов 5015, пользователей - 8, ролей - 15 (рис. 2.4).

```
[dmchistov@dmchistov conf]$ seinfo
```

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:	116257	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 Constrain:	72	MLS Val. Tran:	0
Permissives:	0	Polcap:	5
Defaults:	7	Typebounds:	0
Allowxperm:	0	Neverallowxperm:	0

Рис. 2.4: Статистика по политике

Определяю тип файлов и поддиректорий в /var/www, там лежат файлы Apache типа (рис. 2.5).

```
[dmchistov@dmchistov conf]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Feb 19 23:08 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Feb 19 23:08 html
[dmchistov@dmchistov conf]$
```

Рис. 2.5: Типы файлов в /var/www

Определяю тип файлов в /var/www/html - нету никаких файлов, также определяю круг пользователей, которым разрешено создание файлов этой директории - только root пользователь на такое способен (рис. 2.6).

```
[dmchistov@dmchistov conf]$ ls -lZ /var/www/html
total 0
[dmchistov@dmchistov conf]$ ls -dZ /var/www/html
system_u:object_r:httpd_sys_content_t:s0 /var/www/html
[dmchistov@dmchistov conf]$ ls -ld /var/www/html
drwxr-xr-x. 2 root root 6 Feb 19 23:08 /var/www/html
[dmchistov@dmchistov conf]$
```

Рис. 2.6: Данные по /var/www/html

От имени суперпользователя создаю html файл test.html - простая веб-страница с текстом - test (рис. 2.7).

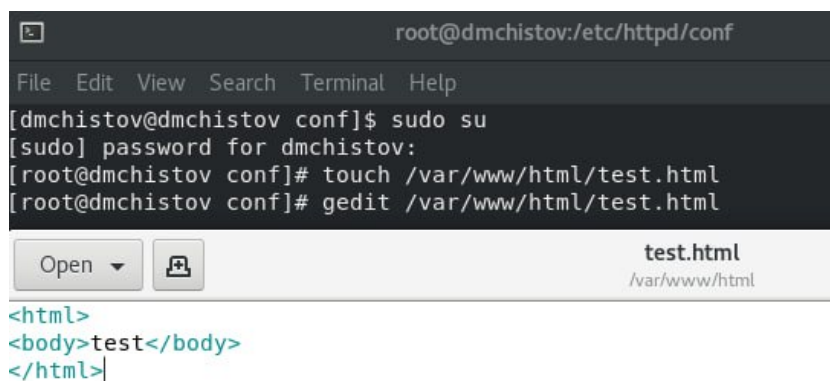


Рис. 2.7: test.html

Проверяю созданный мною файл на контекст - httpd - для Apache (рис. 2.8).

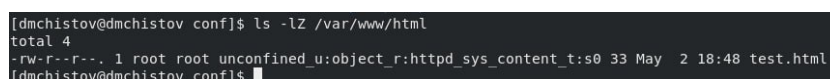


Рис. 2.8: test.html - контекст

Через браузер захожу на эту веб-страничку и вижу соответствующий текст (рис. 2.9).

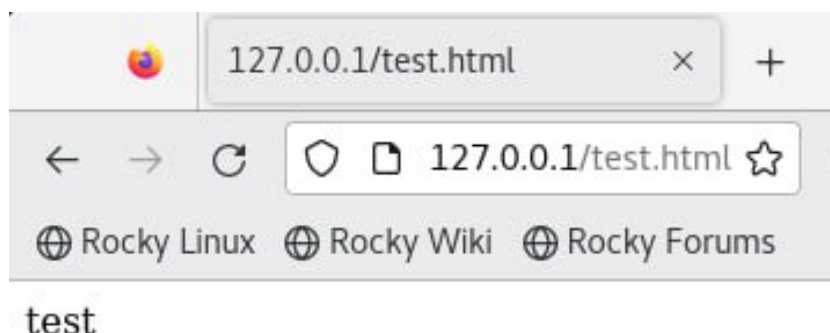


Рис. 2.9: test.html - в браузере

Командой `ls -lZ /var/www/html/test.html` проверяю контекст этого файла - `httpd_sys_content_t` (такой тип позволяет httpd получить доступ к файлу, поэтому мы можем его открыть через браузер) с `unconfined_u` (свободный пользователей) (рис. 2.10).



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

Рис. 2.10: test.html - контекст

Меняю контекст этого файла с httpd\_sys\_content\_t на, например, samba\_share\_t (рис. 2.11).

```
[root@dmchistov conf]# chcon -t samba_share_t /var/www/html/test.html
[root@dmchistov conf]#

[dmchistov@dmchistov conf]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[dmchistov@dmchistov conf]$
```

Рис. 2.11: test.html - новый контекст

Пытаюсь заново обратиться к веб-странице через браузер и получаю отказ (рис. 2.12).

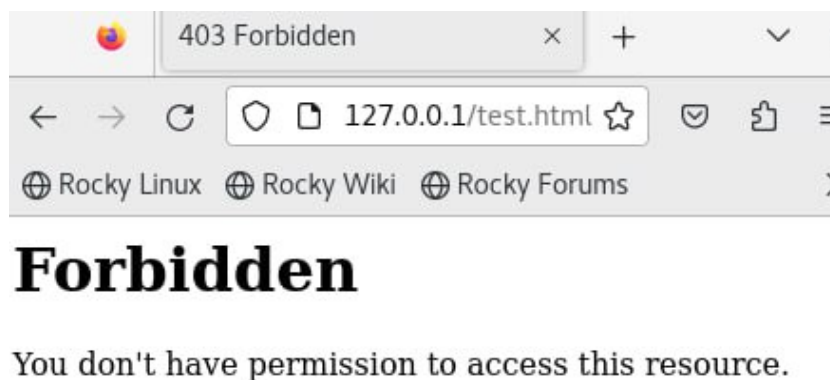


Рис. 2.12: test.html - отказано в доступе

Смотрю лог файлы сервера Apache и пытаюсь разобраться что не так - думаю, дело в том, что мы поменяли тип файла несколькими шагами ранее. Как минимум в логах нас просят поставить какой-то тип данному файлу (рис. 2.13).



```
[root@dmchistov conf]# tail -n1 /var/log/messages
May  2 19:04:37 dmchistov httpd[44872]: Server configured, listening on: port 81
[root@dmchistov conf]#
```

Рис. 2.16: Расследую ситуацию - прослушивание на порте 81

Смотрю другие лог файлы, вижу, что мне говорят об отсутствии прав (рис. 2.17).

```
[root@dmchistov httpd]# cat error_log
[Fri May 02 17:58:22.637712 2025] [core:notice] [pid 41577:tid 139701588023616] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri May 02 17:58:22.638834 2025] [suexec:notice] [pid 41577:tid 139701588023616] AH0222: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri May 02 17:58:22.662345 2025] [lbmethod:heartbeat:notice] [pid 41577:tid 139701588023616] AH02282: No slotmem from mod_heartbeat
[Fri May 02 17:58:22.663210 2025] [http2:warn] [pid 41577:tid 139701588023616] AH02951: mod_ssl does not seem to be enabled
[Fri May 02 17:58:22.666327 2025] [mpm_event:notice] [pid 41577:tid 139701588023616] AH00489: Apache/2.4.37 (Rocky Linux) configured -- resuming normal operations
[Fri May 02 17:58:22.666338 2025] [core:notice] [pid 41577:tid 139701588023616] AH00994: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Fri May 02 18:17:36.012465 2025] [mpm_event:notice] [pid 41577:tid 139701588023616] AH00492: caught SIGTERM, shutting down gracefully
[Fri May 02 18:17:36.111422 2025] [core:notice] [pid 42419:tid 139634997463360] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri May 02 18:17:36.112536 2025] [suexec:notice] [pid 42419:tid 139634997463360] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri May 02 18:17:36.126690 2025] [lbmethod:heartbeat:notice] [pid 42419:tid 139634997463360] AH02282: No slotmem from mod_heartbeat
[Fri May 02 18:17:36.126660 2025] [http2:warn] [pid 42419:tid 139634997463360] AH02951: mod_ssl does not seem to be enabled
[Fri May 02 18:17:36.129142 2025] [mpm_event:notice] [pid 42419:tid 139634997463360] AH00489: Apache/2.4.37 (Rocky Linux) configured -- resuming normal operations
[Fri May 02 18:17:36.129177 2025] [core:notice] [pid 42419:tid 139634997463360] AH00994: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Fri May 02 18:56:04.356406 2025] [core:error] [pid 42430:tid 139634400810752] (13)Permission denied: [client 127.0.0.1:48318] AH00835: access to /test.html denied
[filesystem path "/usr/www/html/test.html"] because search permissions are missing on a component of the path
[Fri May 02 18:57:03.924558 2025] [core:error] [pid 42430:tid 139634400810752] (13)Permission denied: [client 127.0.0.1:48318] AH00835: access to /test.html denied
[filesystem path "/usr/www/html/test.html"] because search permissions are missing on a component of the path
[Fri May 02 19:04:36.883158 2025] [mpm_event:notice] [pid 44872:tid 139876629027136] AH00492: caught SIGTERM, shutting down gracefully
[Fri May 02 19:04:37.933738 2025] [core:notice] [pid 44872:tid 139876629027136] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Fri May 02 19:04:37.935457 2025] [suexec:notice] [pid 44872:tid 139876629027136] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri May 02 19:04:37.939192 2025] [lbmethod:heartbeat:notice] [pid 44872:tid 139876629027136] AH02282: No slotmem from mod_heartbeat
[Fri May 02 19:04:37.952591 2025] [http2:warn] [pid 44872:tid 139876629027136] AH02951: mod_ssl does not seem to be enabled
[Fri May 02 19:04:37.956443 2025] [mpm_event:notice] [pid 44872:tid 139876629027136] AH00489: Apache/2.4.37 (Rocky Linux) configured -- resuming normal operations
[Fri May 02 19:04:37.956474 2025] [core:notice] [pid 44872:tid 139876629027136] AH00994: Command line: '/usr/sbin/httpd -D FOREGROUND'
[root@dmchistov httpd]# cat access_log
127.0.0.1 - - [02/May/2025:18:51:14 +0300] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [02/May/2025:18:51:14 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [02/May/2025:18:57:36 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
127.0.0.1 - - [02/May/2025:18:57:36 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

Рис. 2.17: Расследую ситуацию - отсутствие прав

Командой `semanage port -a -t http_port_t -p tcp 81` добавляю порт 81, затем смотрю появился ли он - конечно появился (рис. 2.18).

```
[root@dmchistov httpd]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@dmchistov httpd]#
[root@dmchistov httpd]# 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@dmchistov httpd]#
[root@dmchistov httpd]# systemctl restart httpd
[root@dmchistov httpd]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2025-05-02 19:23:59 MSK; 1min 56s ago
     Docs: man:httpd.service(8)
  Main PID: 45465 (httpd)
    Status: "Running, listening on: port 81"
     Tasks: 213 (limit: 12238)
    Memory: 33.4M
    CGroup: /system.slice/httpd.service
            └─45465 /usr/sbin/httpd -DFOREGROUND
              └─45468 /usr/sbin/httpd -DFOREGROUND
                └─45469 /usr/sbin/httpd -DFOREGROUND
                  └─45470 /usr/sbin/httpd -DFOREGROUND
                    └─45471 /usr/sbin/httpd -DFOREGROUND

May 02 19:23:59 dmchistov.localdomain systemd[1]: Starting The Apache HTTP Server...
May 02 19:23:59 dmchistov.localdomain systemd[1]: Started The Apache HTTP Server.
May 02 19:23:59 dmchistov.localdomain httpd[45465]: Server configured, listening on: port 81
```

Рис. 2.18: Новый порт - 81

Перезапускаю веб-сервер Apache - всё успешно, нам нужно было объявить ему о новом порте 81, т.к. его не было в списке, а конфиге мы поставили прослушивание этого на тот момент отсутствующего порта. Затем возвращаю нашей

веб-страничке необходимый её тип `httpd_sys_content_t` и через браузер обращаюсь к той же веб-страничке, но через порт 81 (`http://127.0.0.1:81/test.html`) - всё работает - текст виден (рис. 2.19).

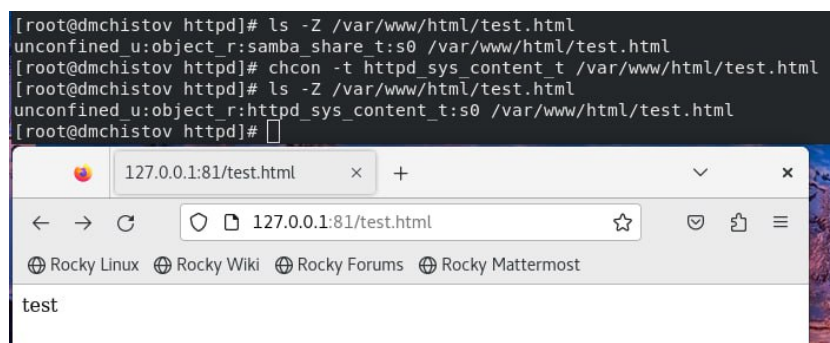


Рис. 2.19: Сайт открывается на порте 81

Завершаю работу - удаляю привязку к порту 81, а также удаляю созданный нами файл `test.html` (рис. 2.20).

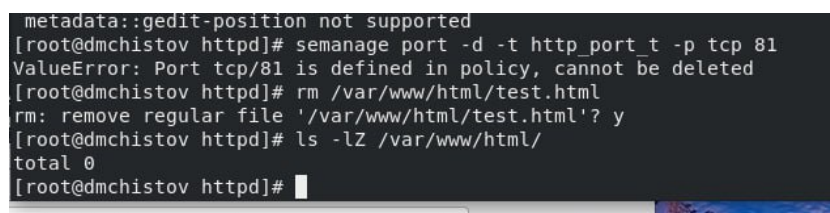


Рис. 2.20: Завершение работы

## **3 Выводы**

В результате выполнения данной лабораторной работы я развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux, проверил работу SELinux на практике совместно с веб-сервером Apache.

## **4 Список литературы**

Лабораторная работа №6