

# Лабораторная работа №6

## Основы информационной безопасности

---

Чистов Д. М.

03 мая 2025

Российский университет дружбы народов, Москва, Россия

Объединённый институт ядерных исследований, Дубна, Россия

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.

## Выполнение лабораторной работы

---

## Выполнение лабораторной работы

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

```
[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.

```
[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: Вывод команды `service httpd status`

Командой `ps auxZ | grep httpd` нахожу процессы веб-сервера Apache и определяю его контекст безопасности - `httpd_t`.

```
[dmchistov@dmchistov conf]$ ps auxZ | 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
[dmchistov@dmchistov conf]$
```

Рис. 3: Процессы Apache

## Выполнение лабораторной работы

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

```
[dmchistov@dmchistov conf]$ sestatus -b | grep httpd
httpd_anon_write off
httpd_built_in_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_sssd off
httpd_dontaudit_search_dirs off
```

## Выполнение лабораторной работы

Командой seinfo смотрю статистику по политике - вижу, что типов 5015, пользователей - 8, ролей - 15.

```
[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
```



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

```
[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. 6: Типы файлов в /var/www

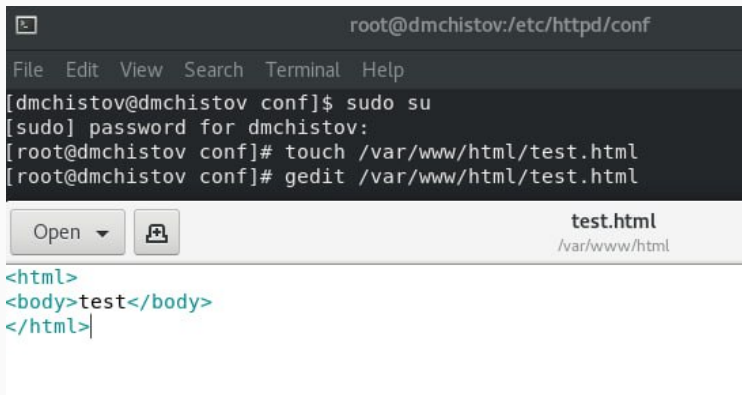
Определяю тип файлов в /var/www/html - нету никаких файлов, также определяю круг пользователей, которым разрешено создание файлов этой директории - только root пользователь на такое способен.

```
[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. 7: Данные по /var/www/html

## Выполнение лабораторной работы

От имени суперпользователя создаю html файл test.html - простая веб-страница с текстом - test.



The image shows a terminal window and a text editor. The terminal window, titled 'root@dmchistov:/etc/httpd/conf', displays the following commands and output:

```
File Edit View Search Terminal Help
[dmchistov@dmchistov conf]$ sudo su
[sudo] password for dmchistov:
[root@dmchistov conf]# touch /var/www/html/test.html
[root@dmchistov conf]# gedit /var/www/html/test.html
```

Below the terminal window, a text editor window titled 'test.html' is shown, displaying the following HTML code:

```
<html>
<body>test</body>
</html>
```

Рис. 8: test.html

Проверяю созданный мною файл на контекст - httpd - для Apache.

```
[dmchistov@dmchistov conf]$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 May  2 18:48 test.html
[dmchistov@dmchistov conf]$
```

Рис. 9: test.html - контекст

## Выполнение лабораторной работы

Через браузер захожу на эту веб-страничку и вижу соответствующий текст.

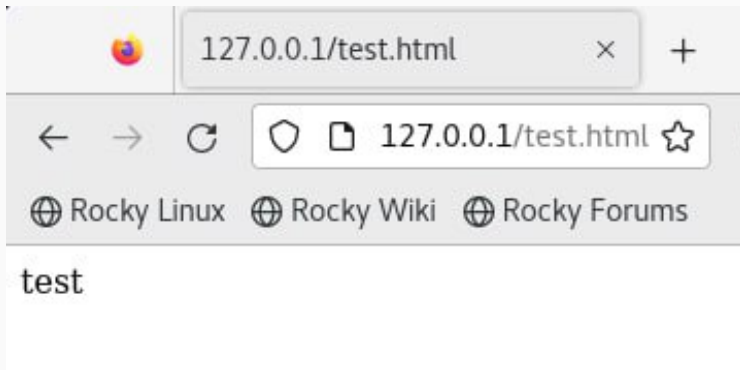
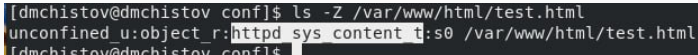


Рис. 10: test.html - в браузере

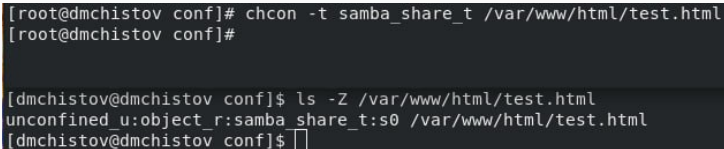
Командой `ls -Z /var/www/html/test.html` проверяю контекст этого файла - `httpd_sys_content_t` (такой тип позволяет `httpd` получить доступ к файлу, поэтому мы можем его открыть через браузер) с `unconfined_u` (свободный пользователей).



```
[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. 11: test.html - контекст

Меняю контекст этого файла с `httpd_sys_content_t` на, например, `samba_share_t`.



```
[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. 12: test.html - новый контекст

Пытаюсь заново обратиться к веб-странице через браузер и получаю отказ.

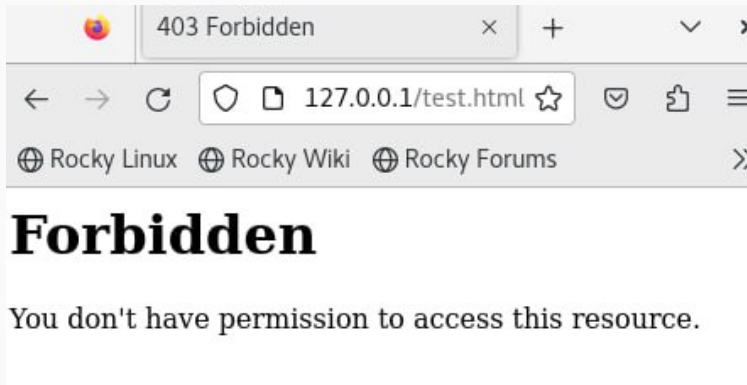


Рис. 13: test.html - отказано в доступе



## Выполнение лабораторной работы

Смотрю лог файлы сервера Arashe 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.

```
[root@dmchistov conf]# tail /var/log/messages
May  2 18:57:31 dmchistov systemd[1]: Started SEtroubleshoot daemon for processing new SELinux denial logs.
May  2 18:57:33 dmchistov setroubleshoot[44677]: failed to retrieve rpm info for /var/www/html/test.html
May  2 18:57:33 dmchistov dbus-daemon[819]: [system] Activating service name='org.fedoraproject.SetroubleshootPrivileged' requested by ':1.636' (uid=984 pid=44677 comm="/usr/libexec/platform-python -Es /usr/sbin/setroub" label="system u:system r:setroubleshootd t:s0") (using servicehelper)
May  2 18:57:34 dmchistov dbus-daemon[819]: [system] Successfully activated service 'org.fedoraproject.SetroubleshootPrivileged'
May  2 18:57:35 dmchistov setroubleshoot[44677]: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SELinux message $ run: sealert -l ae454b3a-dbea-4733-ba44-cd49fd2d2bca
May  2 18:57:35 dmchistov setroubleshoot[44677]: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. 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 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.html to public content t or public content t_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) suggests *****#012#012If you believe that httpd should be allowed getattr 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 now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
May  2 18:57:36 dmchistov setroubleshoot[44677]: failed to retrieve rpm info for /var/www/html/test.html
May  2 18:57:36 dmchistov setroubleshoot[44677]: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html. For complete SELinux message $ run: sealert -l ae454b3a-dbea-4733-ba44-cd49fd2d2bca
May  2 18:57:36 dmchistov setroubleshoot[44677]: SELinux is preventing httpd from getattr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****#012#012If you want to fix the label. #012/var/www/html/test.html default label should be httpd_sys_content_t.#012Then you can run restorecon. 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 confidence) suggests *****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.html to public content t or public content t_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) suggests *****#012#012If you believe that httpd should be allowed getattr 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 now by executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
May  2 18:57:46 dmchistov systemd[1]: setroubleshoot.service: Succeeded
```

Рис. 14: test.html - расследование причины отказа

Запускаю веб-сервер Apache на прослушивании TCP-порта 81, а не 80 - заменяю строку в конфиг файле веб-сервера.

```
# prevent Apache from glomming  
#  
#Listen 12.34.56.78:80  
Listen 81  
  
#
```

Рис. 15: Веб-сервер на прослушивании порта 81

# Выполнение лабораторной работы

Теперь после перезапуска мне не просто отказано в доступе, а сама страничка уже не грузится.

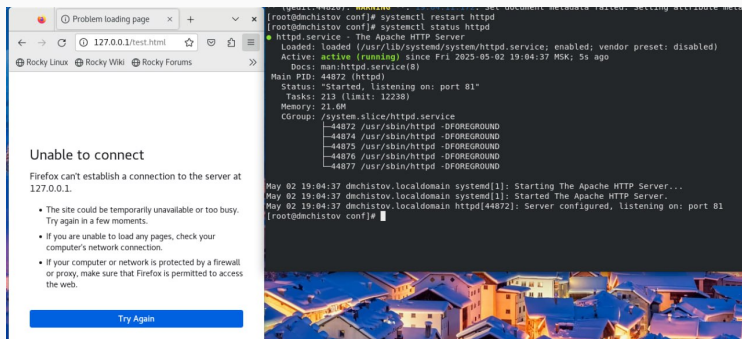


Рис. 16: Веб-сервер не загружает страничку

Смотрю лог файлы - сервер прослушивает порт 81.

A terminal window with a dark background and light-colored text. The prompt is [root@dmchistov conf]#. The command tail -n1 /var/log/messages has been executed. The output shows a log entry from May 2 at 19:04:37 from dmchistov, stating that httpd[44872] is configured and listening on port 81. The prompt is followed by a cursor.

```
[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. 17: Расследую ситуацию - прослушивание на порте 81

Смотрю другие лог файлы, вижу, что мне говорят об отсутствии прав.

```
[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 17:58:22.639824 2025] [suexec:notice] [pid 41577:tid 139701588023616] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri May 02 17:58:22.662345 2025] [lbmethod heartbeat:notice] [pid 41577:tid 139701588023616] AH02282: No slotnen from mod heartnmonitor
[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 17:58:22.666358 2025] [core:notice] [pid 41577:tid 139701588023616] AH00094: Command Line: '/usr/sbin/httpd -D FOREGROUND'
[Fri May 02 18:17:35.012465 2025] [mpm_event:notice] [pid 41577:tid 139701588023616] AH00492: caught SIGWINCH, 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 18:17:36.126850 2025] [lbmethod heartbeat:notice] [pid 42419:tid 139634997463360] AH02282: No slotnen from mod heartnmonitor
[Fri May 02 18:17:36.126860 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] AH00094: 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] AH00035: access to /test.html denied
d (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Fri May 02 18:57:30.264655 2025] [core:error] [pid 42429:tid 1396339334880800] (13)Permission denied: [client 127.0.0.1:60124] AH00035: access to /test.html denied
d (filesystem path '/var/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 SIGWINCH, 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 19:04:37.951921 2025] [lbmethod heartbeat:notice] [pid 44872:tid 139876629027136] AH02282: No slotnen from mod heartnmonitor
[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] AH00094: 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/2025:18:56:04 +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/2025:18:57:30 +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. 18: Расследую ситуацию - отсутствие прав

## Выполнение лабораторной работы

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

```
[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
[root@dmchistov httpd]#
```

## Выполнение лабораторной работы

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.

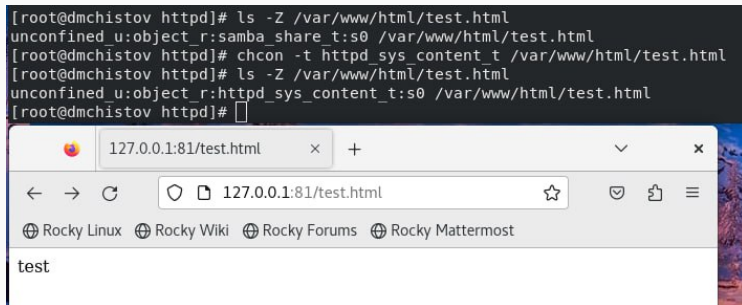
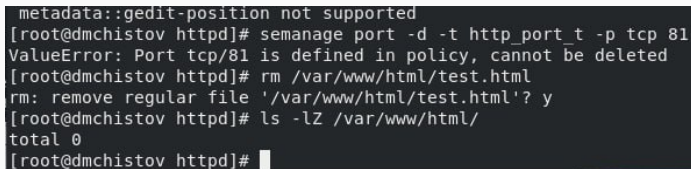


Рис. 20: Сайт открывается на порте 81

Завершаю работу - удаляю привязку к порту 81, а также удаляю созданный нами файл test.html.

A terminal window with a dark background and white text. The text shows the execution of several commands in a root shell on a system named dmchistov. The first command is 'semanage port -d -t http\_port\_t -p tcp 81', which results in an error: 'ValueError: Port tcp/81 is defined in policy, cannot be deleted'. The second command is 'rm /var/www/html/test.html', which results in a confirmation prompt: 'rm: remove regular file '/var/www/html/test.html'? y'. The third command is 'ls -lZ /var/www/html/', which results in 'total 0'. The prompt '[root@dmchistov httpd]#' is visible at the end of each line.

```
metadata::gedit-position not supported
[root@dmchistov httpd]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@dmchistov httpd]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@dmchistov httpd]# ls -lZ /var/www/html/
total 0
[root@dmchistov httpd]#
```

Рис. 21: Завершение работы



## 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.

## Список литературы

---

Лабораторная работа №6