

Отчет к лабораторной работе №6

Common information

discipline: Основы информационной безопасности group: НПМбд-02-21

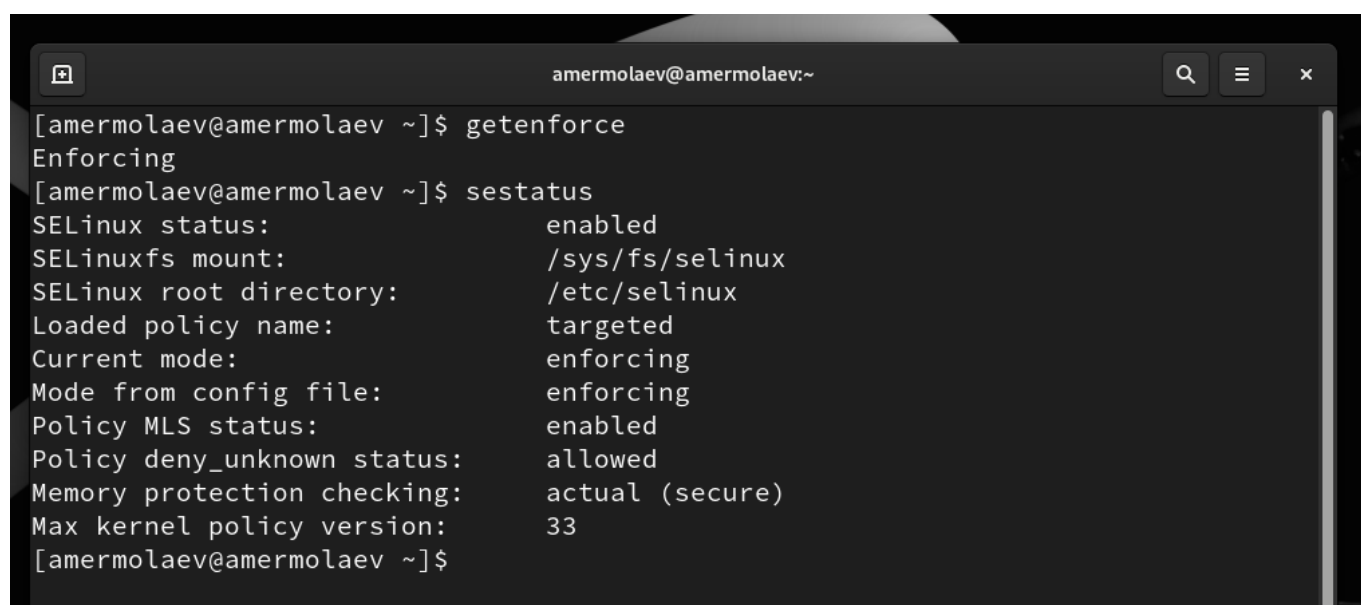
author: Ермолаев А.М.

Цель работы

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

Выполнение работы

Войдем в систему с полученными учётными данными и убедимся, что SELinux работает в режиме enforcing политики targeted с помощью команд **getenforce** и **sestatus**.

A screenshot of a terminal window with a dark background. The window title is 'amermolaev@amermolaev:~'. The terminal shows the following commands and output:

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

Обратим с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедимся, что последний работает (в нашем случае его надо предварительно запустить):

```

[amermolaev@amermolaev ~]$ sudo 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; preset: d
   Active: inactive (dead)
   Docs: man:httpd.service(8)
lines 1-4/4 (END)
[amermolaev@amermolaev ~]$ sudo service httpd start
Redirecting to /bin/systemctl start httpd.service
[amermolaev@amermolaev ~]$ sudo 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; preset: d
   Active: active (running) since Tue 2024-10-08 00:08:12 MSK; 3s ago
   Docs: man:httpd.service(8)
  Main PID: 85402 (httpd)
   Status: "Started, listening on: port 80"

```

Найдем веб-сервер Apache в списке процессов, определим его контекст безопасности:

```

[amermolaev@amermolaev ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0      root      85402  0.0  0.2 20364 11560 ?        Ss   00:08   0:00 /usr/sb
in/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache    85403  0.0  0.1 22096  7528 ?        S    00:08   0:00 /usr/sb
in/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache    85407  0.0  0.2 981520 11308 ?       Sl   00:08   0:00 /usr/sb
in/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache    85408  0.0  0.3 1112656 13756 ?       Sl   00:08   0:00 /usr/sb
in/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache    85409  0.0  0.2 981520 11308 ?       Sl   00:08   0:00 /usr/sb
in/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 amermol+ 85607 0.0  0.0 221664 2432 pts/0 S+  00:09
0:00 grep --color=auto httpd
[amermolaev@amermolaev ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      85402 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      85403 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      85407 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      85408 ?          00:00:00 httpd
system_u:system_r:httpd_t:s0      85409 ?          00:00:00 httpd
[amermolaev@amermolaev ~]$

```

Посмотрим текущее состояние переключателей SELinux для Apache:

```

[amermolaev@amermolaev ~]$ sestatus -b grep 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_yubike               off
awstats_purge_apache_log_files off
boinc_execmem                  on
cdrecord_read_content           off
cluster_can_network_connect    off
cluster_manage_all_files       off
cluster_use_execmem            off
cobbler_anon_write             off
cobbler_can_network_connect    off

```

Посмотрим статистику по политике с помощью команды `seinfo`, также определим множество пользователей, ролей, типов:

```

[amermolaev@amermolaev ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:            33 (MLS enabled)
Target Policy:             selinux
Handle unknown classes:    allow
Classes:                   135
Sensitivities:             1
Types:                     5145
Users:                     8
Booleans:                  356
Allow:                     65504
Auditallow:                176
Type_trans:                271770
Type_member:               37
Role allow:                40
Constraints:               70
MLS Constrain:             72
Permissives:               4
Defaults:                  7
Allowxperm:                0
Auditallowxperm:          0
Ibendportcon:             0
Initial SIDs:              27
Genfscon:                  109
Netifcon:                  0
Permissions:               457
Categories:               1024
Attributes:                259
Roles:                     15
Cond. Expr.:               388
Neverallow:                0
Dontaudit:                 8682
Type_change:               94
Range_trans:               5931
Role_trans:                417
Validatetrans:             0
MLS Val. Tran:             0
Polcap:                    6
Typebounds:                0
Neverallowxperm:          0
Dontauditxperm:           0
Ibpkeycon:                 0
Fs_use:                    35
Portcon:                   665
Nodecon:                   0

```

Определим типы файлов и поддиректорий, находящихся в директории `/var/www`, `/var/www/html`, а также круг пользователей, которым разрешено создание файлов в директории `/var/www/html`:

```
amermolaev@amermolaev:~$ 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
[amermolaev@amermolaev ~]$
[amermolaev@amermolaev ~]$ ls -lZ /var/www/html
total 0
[amermolaev@amermolaev ~]$ ls -lah /var/www
total 4.0K
drwxr-xr-x. 4 root root 33 Oct  8 00:07 .
drwxr-xr-x. 21 root root 4.0K Oct  8 00:07 ..
drwxr-xr-x. 2 root root 6 Aug  8 19:30 cgi-bin
drwxr-xr-x. 2 root root 6 Aug  8 19:30 html
[amermolaev@amermolaev ~]$
```

Создадим от имени суперпользователя html-файл /var/www/html/test.html:

```
amermolaev@amermolaev:~$ sudo nano /var/www/html/test.html
[sudo] password for amermolaev:
[amermolaev@amermolaev ~]$ cat /var/www/html/test.html
<html>
<body>test</body>
</html>
[amermolaev@amermolaev ~]$
```

Проверим контекст созданного файла:

```
amermolaev@amermolaev:~$ ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 Oct  8 00:17 test.html
[amermolaev@amermolaev ~]$
```

Обратимся к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>:

```
Rocky Linux x 127.0.0.1/test.html x +
127.0.0.1/test.html
Rocky Linux Rocky Wiki Rocky Forums Rocky Mattermost Rocky Reddit
test
```

Изучим справку man httpd_selinux. Проверим контекст файла:

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

Изменим контекст файла /var/www/html/test.html с httpd_sys_content_t на любой другой, к которому процесс httpd не должен иметь доступа, например, на samba_share_t:

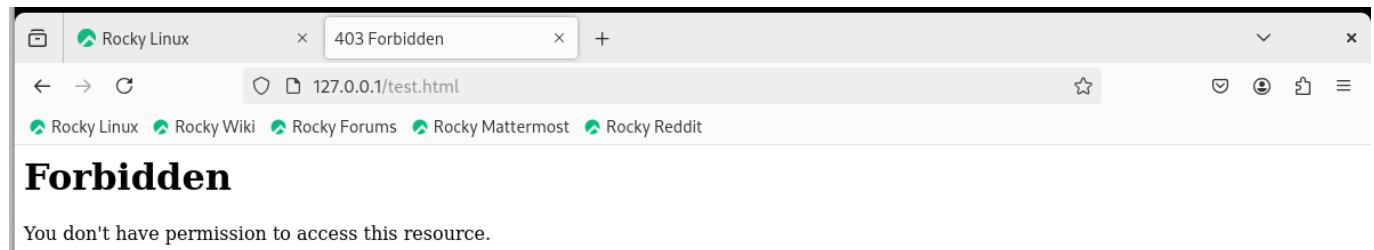
```

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

```

Попробуем ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес

<http://127.0.0.1/test.html>:



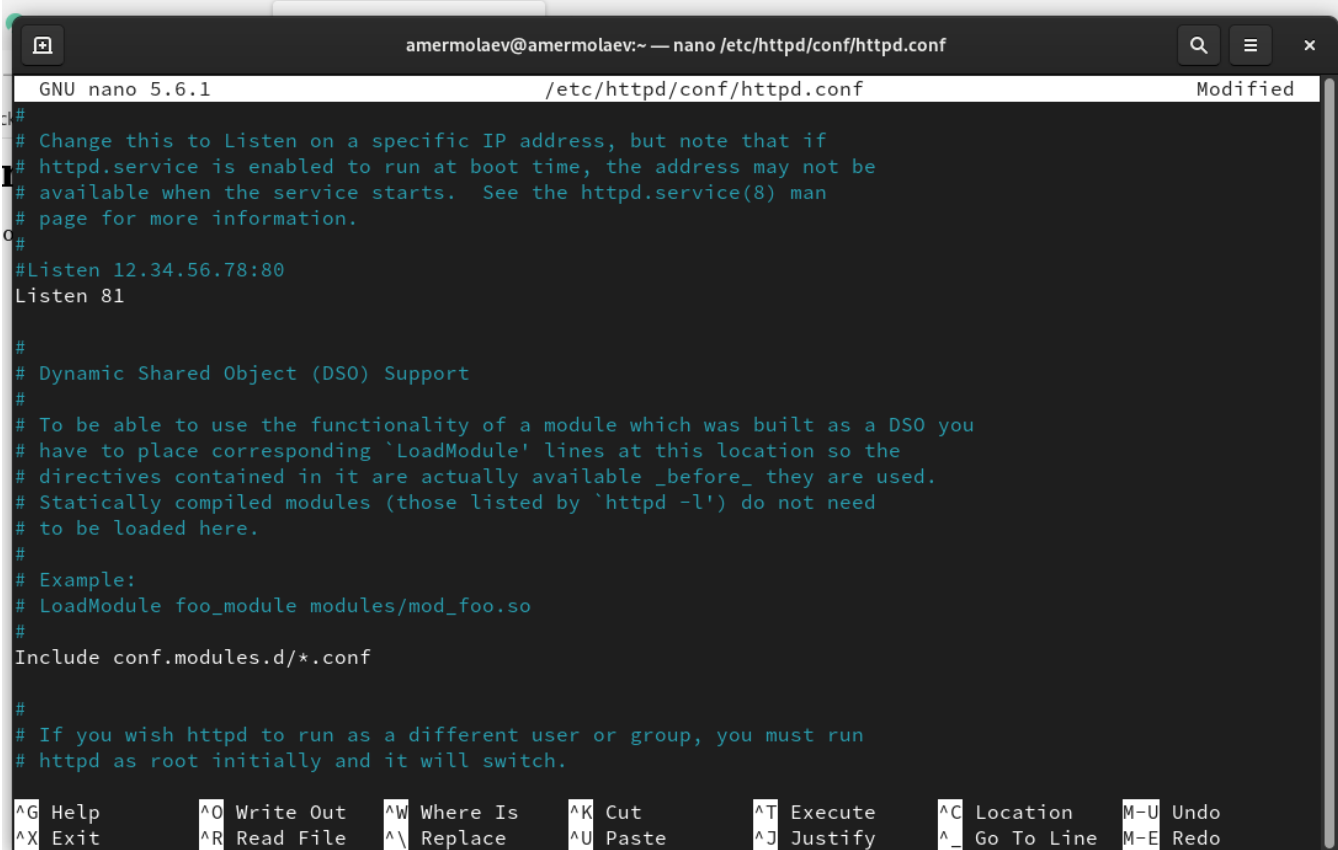
Просмотрим log-файлы веб-сервера Apache и системный лог-файл:

```

[amermolaev@amermolaev ~]$ ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Oct  8 00:17 /var/www/html/test.html
[amermolaev@amermolaev ~]$ sudo tail /var/log/httpd/access_log
127.0.0.1 - - [08/Oct/2024:00:19:53 +0300] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
127.0.0.1 - - [08/Oct/2024:00:19:53 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "http://127.0.0.1/test.html" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
127.0.0.1 - - [08/Oct/2024:00:23:27 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
127.0.0.1 - - [08/Oct/2024:00:23:27 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
127.0.0.1 - - [08/Oct/2024:00:23:28 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
[amermolaev@amermolaev ~]$ sudo tail /var/log/messages
Oct  8 00:23:31 amermolaev setroubleshoot[86471]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l fd94aefa-9721-4d61-9e63-c01d1f7dde84
Oct  8 00:23:31 amermolaev setroubleshoot[86471]: SELinux is preventing /usr/sbin/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_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-ht

```

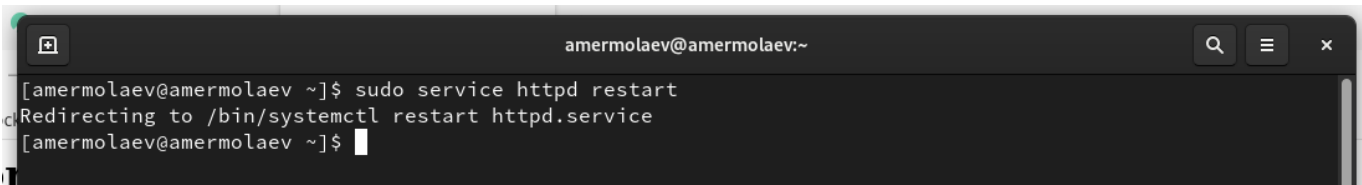
Попробуем запустить веб-сервер Apache на прослушивание TCP-порта 81 Для этого в файле `/etc/httpd/httpd.conf` найдем строчку `Listen 80` и заменим её на `Listen 81`:



```
amercolaev@amercolaev:~ — nano /etc/httpd/conf/httpd.conf
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf Modified
#
# Change this to Listen on a specific IP address, but note that if
# httpd.service is enabled to run at boot time, the address may not be
# available when the service starts. See the httpd.service(8) man
# page for more information.
#
#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.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
Include conf.modules.d/*.conf
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.

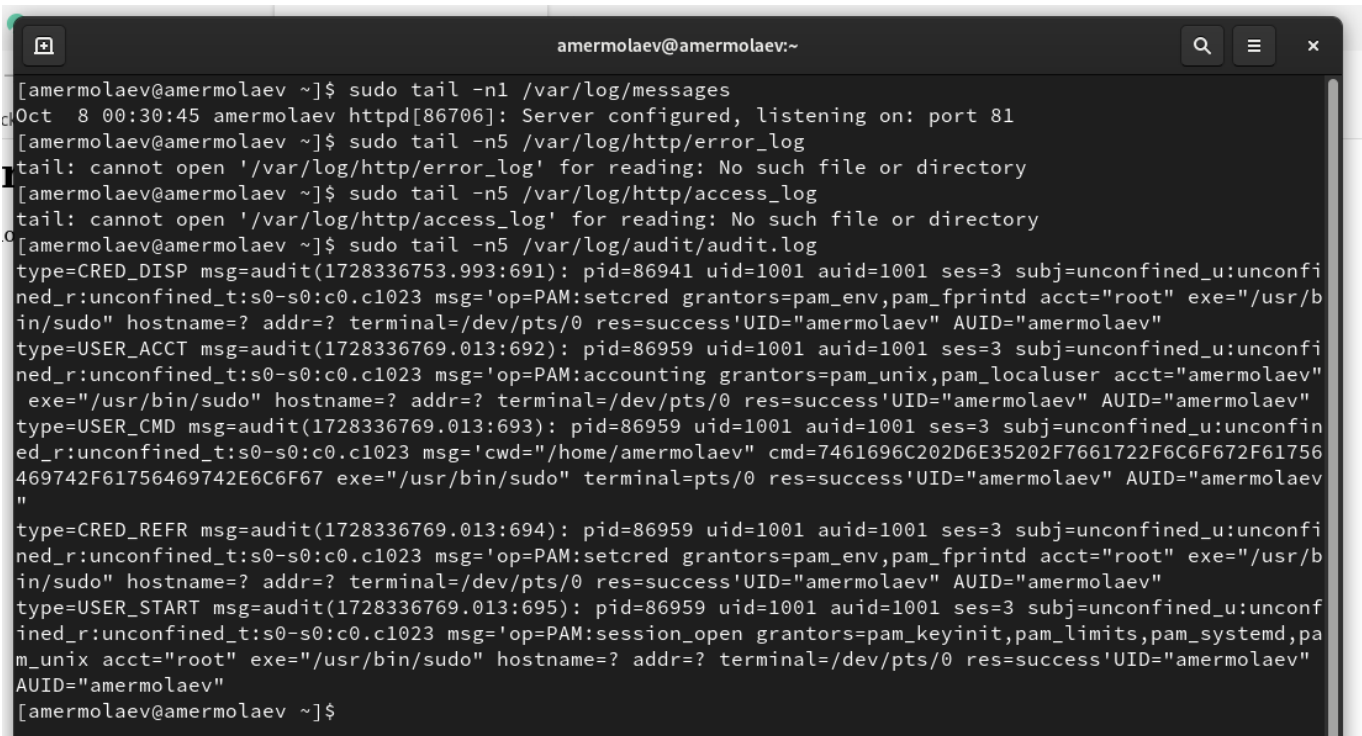
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo
```

Выполним перезапуск веб-сервера Apache:



```
amercolaev@amercolaev:~
[amercolaev@amercolaev ~]$ sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[amercolaev@amercolaev ~]$
```

Проанализируем лог-файлы:



```
amercolaev@amercolaev:~
[amercolaev@amercolaev ~]$ sudo tail -n1 /var/log/messages
Oct 8 00:30:45 amercolaev httpd[86706]: Server configured, listening on: port 81
[amercolaev@amercolaev ~]$ sudo tail -n5 /var/log/http/error_log
tail: cannot open '/var/log/http/error_log' for reading: No such file or directory
[amercolaev@amercolaev ~]$ sudo tail -n5 /var/log/http/access_log
tail: cannot open '/var/log/http/access_log' for reading: No such file or directory
[amercolaev@amercolaev ~]$ sudo tail -n5 /var/log/audit/audit.log
type=CRED_DISP msg=audit(1728336753.993:691): pid=86941 uid=1001 auid=1001 ses=3 subj=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/b
in/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="amercolaev" AUID="amercolaev"
type=USER_ACCT msg=audit(1728336769.013:692): pid=86959 uid=1001 auid=1001 ses=3 subj=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser acct="amercolaev"
exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="amercolaev" AUID="amercolaev"
type=USER_CMD msg=audit(1728336769.013:693): pid=86959 uid=1001 auid=1001 ses=3 subj=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023 msg='cwd="/home/amercolaev" cmd=7461696C202D6E35202F7661722F6C6F672F61756
469742F61756469742E6C6F67 exe="/usr/bin/sudo" terminal=pts/0 res=success'UID="amercolaev" AUID="amercolaev"
type=CRED_REFR msg=audit(1728336769.013:694): pid=86959 uid=1001 auid=1001 ses=3 subj=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_env,pam_fprintd acct="root" exe="/usr/b
in/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="amercolaev" AUID="amercolaev"
type=USER_START msg=audit(1728336769.013:695): pid=86959 uid=1001 auid=1001 ses=3 subj=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_systemd,pa
m_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'UID="amercolaev"
AUID="amercolaev"
[amercolaev@amercolaev ~]$
```

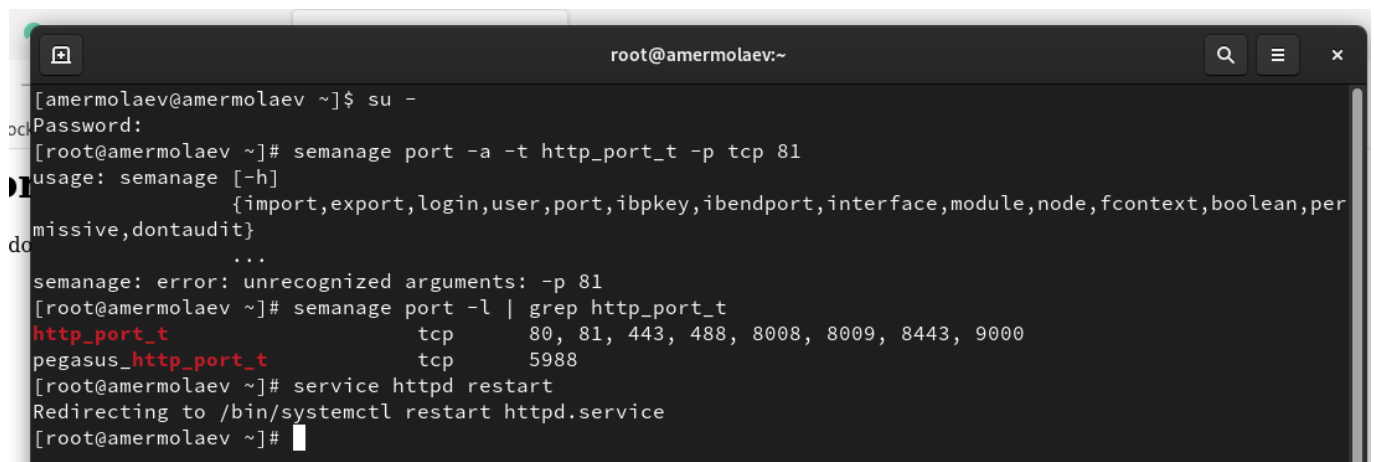
Выполним команду

```
semanage port -a -t http_port_t -p tcp 81
```

После этого проверим список портов командой

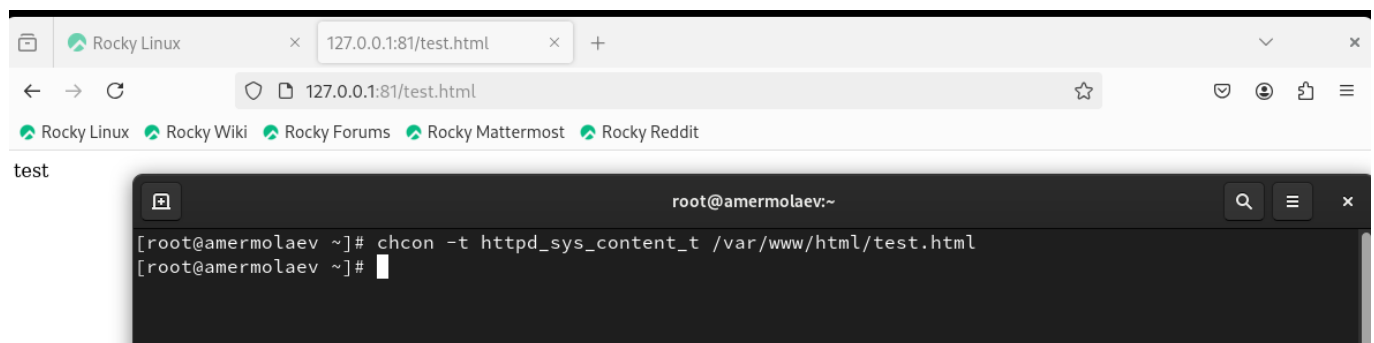
```
semanage port -l | grep http_port_t
```

После чего попробуем запустить веб-сервер Apache ещё раз:



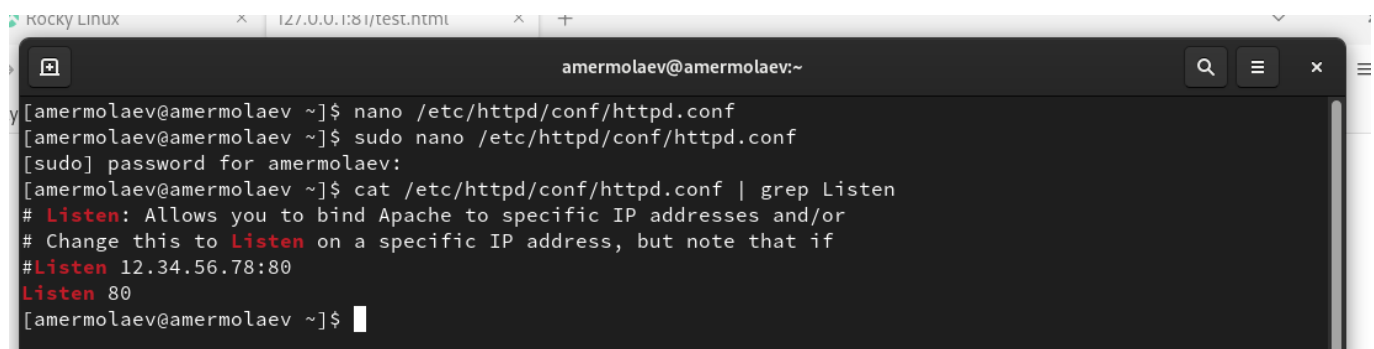
```
root@amermolaev:~  
[amermolaev@amermolaev ~]$ su -  
Password:  
[root@amermolaev ~]# semanage port -a -t http_port_t -p tcp 81  
usage: semanage [-h]  
                {import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,per  
missive,dontaudit}  
                ...  
semanage: error: unrecognized arguments: -p 81  
[root@amermolaev ~]# 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@amermolaev ~]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[root@amermolaev ~]#
```

Вернем контекст httpd_sys_content_t к файлу /var/www/html/ test.html:



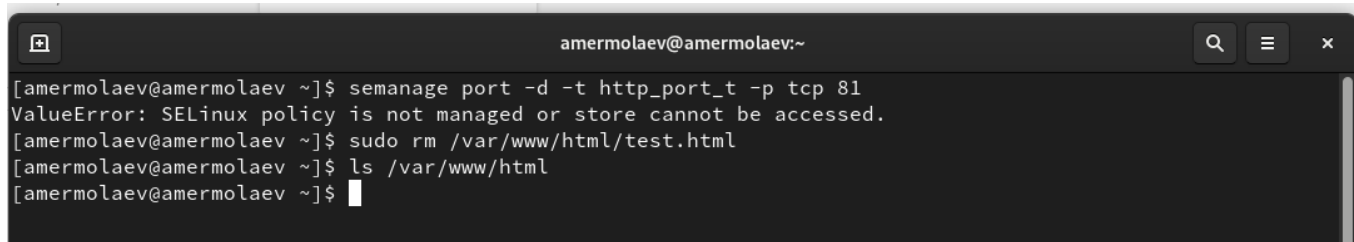
```
Rocky Linux x 127.0.0.1:81/test.html x +  
test  
root@amermolaev:~  
[root@amermolaev ~]# chcon -t httpd_sys_content_t /var/www/html/test.html  
[root@amermolaev ~]#
```

Исправим конфигурационный файл apache, вернув Listen 80.



```
Rocky Linux x 127.0.0.1:81/test.html x +  
amermolaev@amermolaev:~  
[amermolaev@amermolaev ~]$ nano /etc/httpd/conf/httpd.conf  
[amermolaev@amermolaev ~]$ sudo nano /etc/httpd/conf/httpd.conf  
[sudo] password for amermolaev:  
[amermolaev@amermolaev ~]$ cat /etc/httpd/conf/httpd.conf | grep Listen  
# Listen: Allows you to bind Apache to specific IP addresses and/or  
# Change this to Listen on a specific IP address, but note that if  
# Listen 12.34.56.78:80  
Listen 80  
[amermolaev@amermolaev ~]$
```

Удалим привязку http_port_t к 81 порту. Затем удалим файл /var/www/html/test.html:

A terminal window with a dark background and light text. The title bar shows 'amermolaev@amermolaev:~'. The terminal content shows a sequence of commands and their outputs: 'semanage port -d -t http_port_t -p tcp 81' results in a 'ValueError: SELinux policy is not managed or store cannot be accessed.'; 'sudo rm /var/www/html/test.html' is executed successfully; and 'ls /var/www/html' is also executed successfully, with a cursor visible at the end of the line.

```
amermolaev@amermolaev:~  
[amermolaev@amermolaev ~]$ semanage port -d -t http_port_t -p tcp 81  
ValueError: SELinux policy is not managed or store cannot be accessed.  
[amermolaev@amermolaev ~]$ sudo rm /var/www/html/test.html  
[amermolaev@amermolaev ~]$ ls /var/www/html  
[amermolaev@amermolaev ~]$
```

Вывод

В рамках выполнения работы я

- Развил навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux
- Проверил работу SELinux на практике совместно с веб-сервером Apache.

Список литературы

- <https://rockylinux.org/>
- <https://habr.com/ru/articles/469667/>
- <https://www.linuxteck.com/how-to-install-apache-on-rocky-linux/>
- <https://habr.com/ru/companies/kingservers/articles/209644/>