

Презентация по лабораторной работе №6

Основы информационной безопасности

Петрова А.А.

01 мая 2025

Российский университет дружбы народов, Москва, Россия

Информация

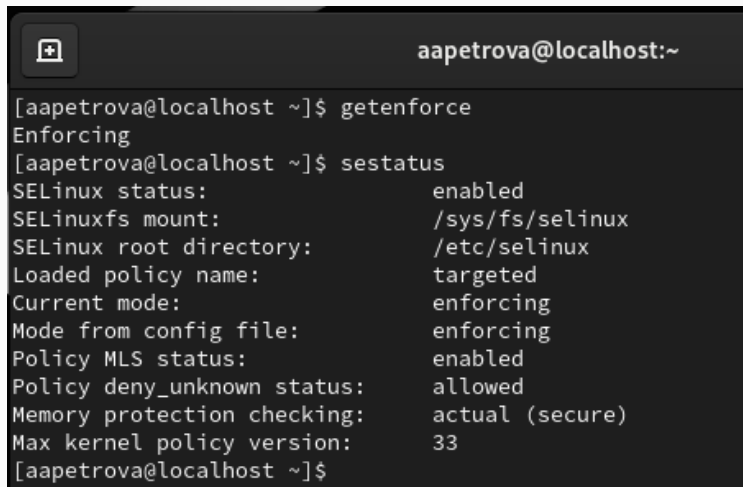
- Петрова Алевтина Александровна
- студентка группы НКАбд-04-23
- Российский университет дружбы народов

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

Выполнение лабораторной работы

Выполнение лабораторной работы

SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`

A terminal window with a dark background. The title bar shows a window icon and the text 'aapetrova@localhost:~'. The terminal content shows the execution of 'getenforce' and 'sestatus' commands. The output of 'sestatus' is a key-value list of SELinux configuration details.

```
aapetrova@localhost:~  
[aapetrova@localhost ~]$ getenforce  
Enforcing  
[aapetrova@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  
[aapetrova@localhost ~]$
```

Выполнение лабораторной работы

Запускаю сервер apache, далее обращаюсь с помощью браузера к веб-серверу, запущенному на компьютере, он работает, что видно из вывода команды `service httpd status`

```
[aapetrova@localhost ~]$ sudo systemctl start httpd
[sudo] пароль для aapetrova:
[aapetrova@localhost ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[aapetrova@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; preset: disabled)
   Active: active (running) since Tue 2025-04-29 19:13:44 MSK; 13s ago
     Docs: man:httpd.service(8)
   Main PID: 97977 (httpd)
    Status: "Total requests: 0; Idle/Busy workers 100/0; Requests/sec: 0; Bytes served/sec: 0"
      Tasks: 177 (limit: 12175)
    Memory: 28.4M
       CPU: 104ms
    CGroup: /system.slice/httpd.service
            └─97977 /usr/sbin/httpd -DFOREGROUND
              └─97978 /usr/sbin/httpd -DFOREGROUND
                └─97979 /usr/sbin/httpd -DFOREGROUND
                  └─97980 /usr/sbin/httpd -DFOREGROUND
```

Выполнение лабораторной работы

С помощью команды `ps auxZ | grep httpd` нашла веб-сервер Apache в списке процессов. Его контекст безопасности - `httpd_t`

```
[aapetrova@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0      root      97977  0.0  0.5  21024 11272 ?
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache    97978  0.0  0.3   22900   7136 ?
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache    97979  0.0  0.6  2358644 13192 ?
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache    97980  0.0  0.6  2161972 12952 ?
0 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache    97981  0.0  0.7  2161972 14868 ?
0 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 aapetro+  98218  0.0  0.
+ 19:17  0:00 grep --color=auto httpd
[aapetrova@localhost ~]$
```

Рис. 3: Контекст безопасности Apache

Выполнение лабораторной работы

Просмотрела текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd`

```
[aapetrova@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
```

Выполнение лабораторной работы

Просмотрела статистику по политике с помощью команды `seinfo`. Множество пользователей - 8, ролей - 39, типов - 5135.

```
[aapetrova@localhost ~]$ 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:                    5169     Attributes:               259
Users:                    8         Roles:                    15
Booleans:                 358      Cond. Expr.:             390
Allow:                    65633     Neverallow:               0
Auditallow:               176      Dontaudit:               8703
Type_trans:               271851   Type_change:              94
Type_member:               37       Range_trans:             5931
Role allow:                40       Role_trans:               417
Constraints:               70       Validatetrans:            0
MLS Constrains:           72       MLS Val. Tran:            0
```

Типы поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www` следующие: владелец - `root`, права на изменения только у владельца. Файлов в директории нет

```
[aapetrova@localhost ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 янв 22 03:25 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0      6 янв 22 03:25 html
[aapetrova@localhost ~]$
```

Рис. 6: Типы поддиректорий

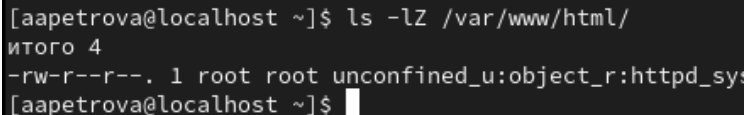
Выполнение лабораторной работы

Создать файл может только суперпользователь, поэтому от его имени создаем файл touch.html со следующим содержанием:

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

Рис. 7: Создание файла

Проверяю контекст созданного файла. По умолчанию это httpd_sys_content_t

A terminal window with a dark background and light gray text. The prompt is [aapetrova@localhost ~]\$. The command ls -lZ /var/www/html/ is entered. The output shows 'итого 4' followed by a line of permissions: '-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t /var/www/html/00000000.html'. The prompt is then shown again with a cursor.

```
[aapetrova@localhost ~]$ ls -lZ /var/www/html/  
итого 4  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t /var/www/html/00000000.html  
[aapetrova@localhost ~]$
```

Рис. 8: Контекст файла

Выполнение лабораторной работы

Обращаюсь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Файл был успешно отображён

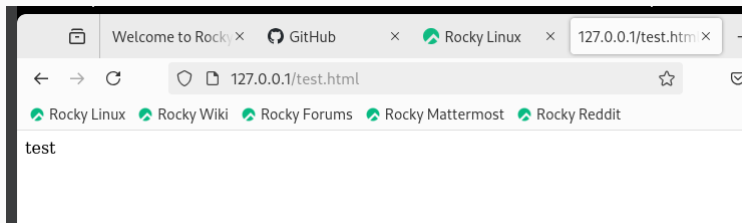
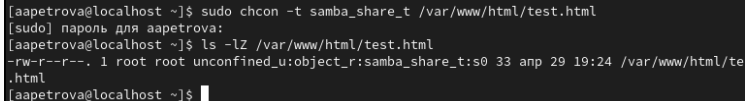


Рис. 9: Отображение файла

Изменяю 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`: `chcon -t samba_share_t /var/www/html/test.html` `ls -Z /var/www/html/test.html` Контекст действительно поменялся



```
[aapetrova@localhost ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] пароль для aapetrova:
[aapetrova@localhost ~]$ ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 anp 29 19:24 /var/www/html/test.html
[aapetrova@localhost ~]$
```

Рис. 10: Изменение контекста

Выполнение лабораторной работы

При попытке отображения файла в браузере получаем сообщение об ошибке файл не был отображён, хотя права доступа позволяют читать этот файл любому пользователю, потому что установлен контекст, к которому процесс `httpd` не должен иметь доступа.

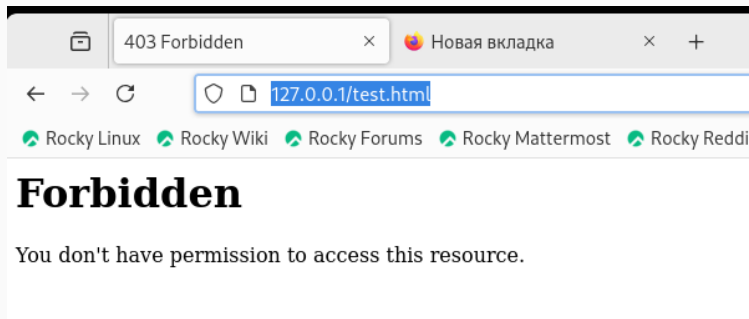


Рис. 11: Отображение файла

Выполнение лабораторной работы

Чтобы запустить веб-сервер Apache на прослушивание TCP-порта 81 открываю файл `/etc/httpd/httpd.conf` для изменения. Нахожу строчку `Listen 80` и заменяю её на `Listen 81`.

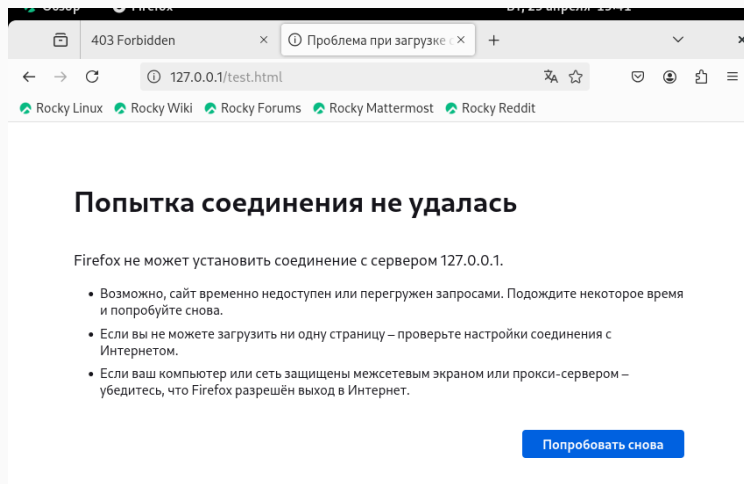


```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
#Listen 12.34.56.78:80
;tListen 81

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are
# 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

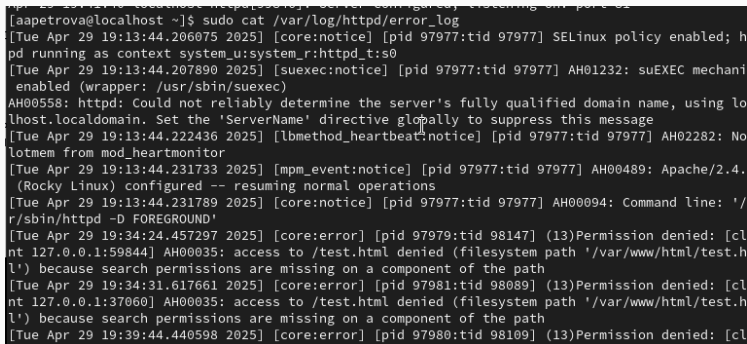
#
# If you wish httpd to run as a different user or group, you must run
```

Выполняю перезапуск веб-сервера Apache. Произошёл сбой



Выполнение лабораторной работы

Просмотрите файлы `/var/log/httpd/error_log`, `/var/log/httpd/access_log` и `/var/log/audit/audit.log` и выясните, в каких файлах появились записи. Запись появилась в файлу `error_log`

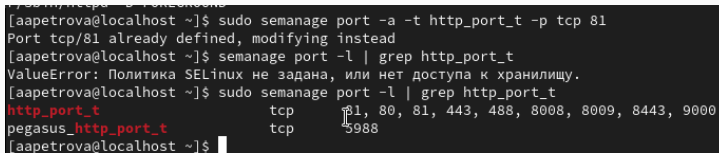


```
[aapetrova@localhost ~]$ sudo cat /var/log/httpd/error_log
[Tue Apr 29 19:13:44.206075 2025] [core:notice] [pid 97977:tid 97977] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Tue Apr 29 19:13:44.207890 2025] [suexec:notice] [pid 97977:tid 97977] AH01232: suEXEC mechanism 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 suppress this message
[Tue Apr 29 19:13:44.222436 2025] [lbmethod_heartbeat:notice] [pid 97977:tid 97977] AH02282: No lotmem from mod_heartbeat
[Tue Apr 29 19:13:44.231733 2025] [mpm_event:notice] [pid 97977:tid 97977] AH00489: Apache/2.4. (Rocky Linux) configured -- resuming normal operations
[Tue Apr 29 19:13:44.231789 2025] [core:notice] [pid 97977:tid 97977] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Tue Apr 29 19:34:24.457297 2025] [core:error] [pid 97979:tid 98147] (13)Permission denied: [client 127.0.0.1:59844] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Tue Apr 29 19:34:31.617661 2025] [core:error] [pid 97981:tid 98089] (13)Permission denied: [client 127.0.0.1:37060] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Tue Apr 29 19:39:44.440598 2025] [core:error] [pid 97980:tid 98109] (13)Permission denied: [client 127.0.0.1:59844] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
```

Рис. 14: Проверка лог-файлов

Выполнение лабораторной работы

Выполняю команду `semanage port -a -t http_port_t -p tcp 81` После этого проверяю список портов командой `semanage port -l | grep http_port_t`
Порт 81 появился в списке



```
[aapetrova@localhost ~]$ sudo semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[aapetrova@localhost ~]$ semanage port -l | grep http_port_t
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[aapetrova@localhost ~]$ sudo 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
```

Рис. 15: Проверка портов

Перезапускаю сервер Apache

A terminal window with a dark background and light-colored text. The prompt is [aapetrova@localhost ~]. The first command is sudo systemctl restart httpd. The second command is sudo chcon -t httpd_sys_content_t /var/www/html/test.html. The third command is sudo systemctl restart httpd. The prompt is followed by a cursor.

```
pegasus_http_port_t      tcp      5988  
[aapetrova@localhost ~]$ sudo systemctl restart httpd  
[aapetrova@localhost ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test.html  
[aapetrova@localhost ~]$ sudo systemctl restart httpd  
[aapetrova@localhost ~]$
```

Рис. 16: Перезапуск сервера

Выполнение лабораторной работы

Теперь он работает, ведь мы внесли порт 81 в список портов `httpd_port_t`

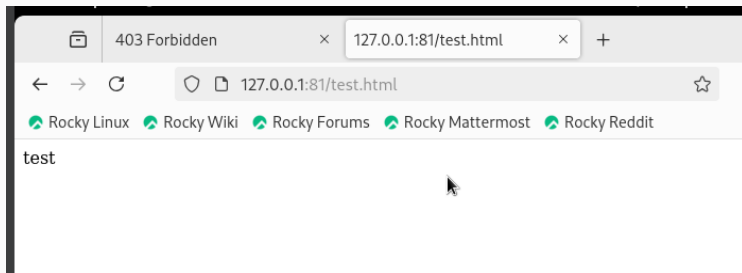
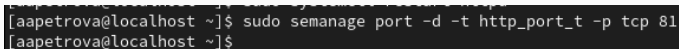


Рис. 17: Проверка сервера

Возвращаю в файле `/etc/httpd/httpd.conf` порт 80, вместо 81. Проверяю, что порт 81 удален, это правда.

A terminal window with a dark background and light text. The prompt is [aapetrova@localhost ~]. The command entered is sudo semanage port -d -t http_port_t -p tcp 81. The output is [aapetrova@localhost ~]\$.

```
[aapetrova@localhost ~]$ sudo semanage port -d -t http_port_t -p tcp 81
[aapetrova@localhost ~]$
```

Рис. 18: Проверка порта 81

Далее удаляю файл test.html, проверяю, что он удален

```
[aapetrova@localhost ~]$ rm /var/www/html/test.html
rm: удалить защищённый от записи обычный файл '/var/www/html/test.html'? y
rm: невозможно удалить '/var/www/html/test.html': Отказано в доступе
[aapetrova@localhost ~]$ sudo rm /var/www/html/test.html
[aapetrova@localhost ~]$ ls -lZ /var/www/html
итого 0
[aapetrova@localhost ~]$
```

Рис. 19: 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.

...