Лабораторная работа №6

Андрианова Марина Георгиевна
RUDN University, Moscow,
Russian Federation
2024, 10 October

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 лабораторной работы

• Вошла в систему под своей учетной записью. Убедилась, что SELinux работает в режиме enforcing политики targeted с помощью команд getenforce и sestatus (рис. [-@fig:001]).

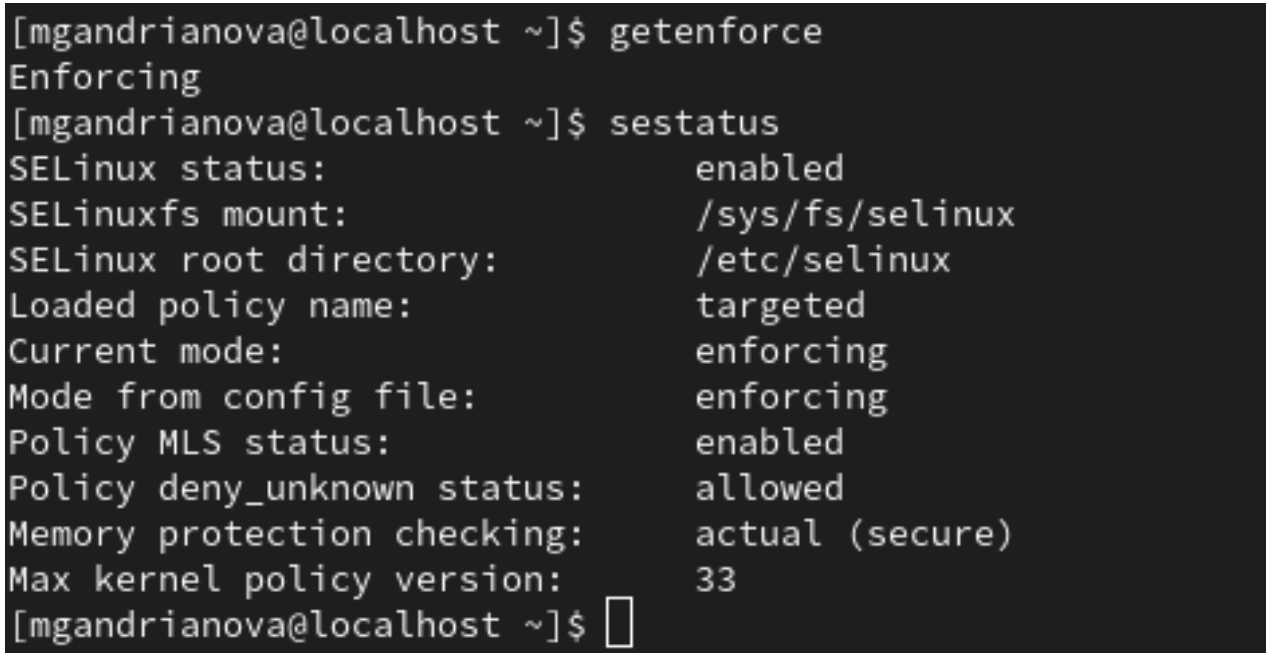

Рис.1. Проверка режима работы SELinux

Запускаю сервер apache, далее обращаюсь с помощью браузера к веб-серверу, запущенному на компьютере, он работает, что видно из вывода команды `service httpd status` (рис. [-@fig:002]).

```
[mgandrianova@localhost ~]$ sudo systemctl start httpd
[sudo] пароль для mgandrianova:
[mgandrianova@localhost ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[mgandrianova@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 Wed 2024-10-09 21:10:51 MSK; 1min 29s ago
       Docs: man:httpd.service(8)
   Main PID: 2860 (httpd)
     Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec:   0 B/sec"
      Tasks: 177 (limit: 10980)
     Memory: 38.2M
        CPU: 727ms
     CGroup: /system.slice/httpd.service
             ├─2860 /usr/sbin/httpd -DFOREGROUND
             ├─2861 /usr/sbin/httpd -DFOREGROUND
             ├─2862 /usr/sbin/httpd -DFOREGROUND
             ├─2863 /usr/sbin/httpd -DFOREGROUND
             └─2868 /usr/sbin/httpd -DFOREGROUND

окт 09 21:10:50 localhost.localdomain systemd[1]: Starting The Apache HTTP Server...
окт 09 21:10:50 localhost.localdomain httpd[2860]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.loc>
окт 09 21:10:51 localhost.localdomain systemd[1]: Started The Apache HTTP Server.
окт 09 21:10:51 localhost.localdomain httpd[2860]: Server configured, listening on: port 80
lines 1-20/20 (END)
```

Рис.2. Проверка работы Apache

С помощью команды `ps auxZ | grep httpd` нашла веб-сервер Apache в списке процессов. Его контекст безопасности - httpd_t (рис. [-@fig:003]).

```
[mgandrianova@localhost ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root        2860  0.1  0.6  20152 11432 ?        Ss   21:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      2861  0.0  0.4  22032  7356 ?        S    21:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      2862  0.1  0.9 1112588 17612 ?       Sl   21:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      2863  0.0  0.8 981452 15340 ?        Sl   21:10   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache      2868  0.1  0.8 981452 15344 ?        Sl   21:10   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 mgandri+ 3132 0.0  0.1 221688 2560 pts/0 S+ 21:14   0:00 grep --color=auto httpd
[mgandrianova@localhost ~]$
```

Рис.3. Контекст безопасности Apache

В директории /var/www/html нет файлов. (рис. [-@fig:004]).

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

Рис.4. Типы файлов

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

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

(рис. [-@fig:005]).

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

Рис.5. Создание файла

Проверяю контекст созданного файла. По умолчанию это httpd_sys_content_t (рис. [-@fig:006]).

```
[mgandrianova@localhost ~]$ ls -lZ /var/www/html/
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 33 окт  9 21:22 test.html
```

Рис.6. Контекст файла

Обращаюсь к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Файл был успешно отображён (рис. [-@fig:007]).

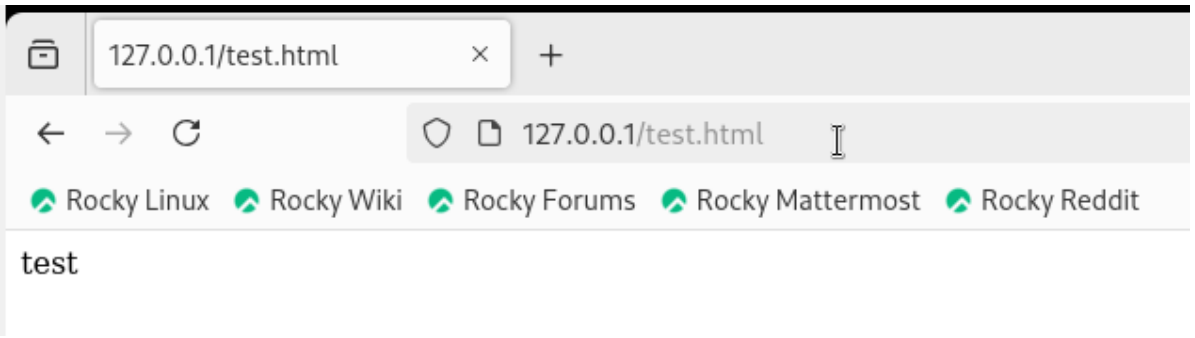

Рис.7. Отображение файла

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

```
chcon -t samba_share_t /var/www/html/test.html
ls -Z /var/www/html/test.html
```

Контекст действительно поменялся (рис. [-@fig:008]).

```
[mgandrianova@localhost ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sudo] пароль для mgandrianova:
[mgandrianova@localhost ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Рис.8. Изменение контекста

При попытке отображения файла в браузере получаем сообщение об ошибке (рис. [-@fig:009]).

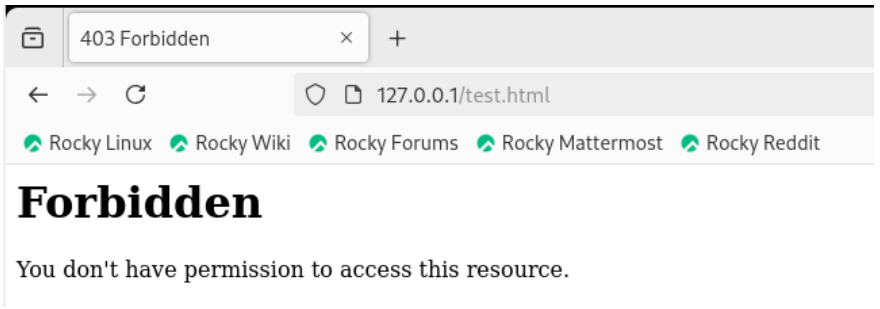

Рис.9. Отображение файла

Чтобы запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services) открываю файл /etc/httpd/httpd.conf для изменения (рис. [-@fig:010]).

Рис.10. Изменение файла

Нахожу строчку Listen 80 и заменяю её на Listen 81 (рис. [-@fig:011]).

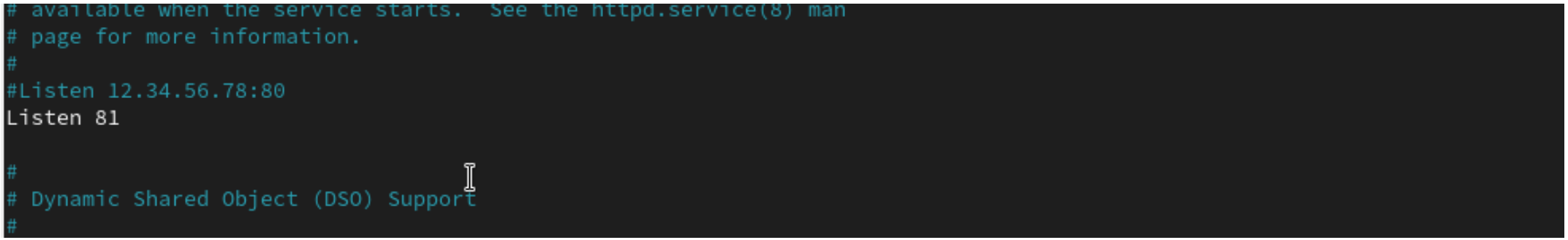

Рис.11. Изменение порта

Выполняю перезапуск веб-сервера Apache. Произошёл сбой, потому что порт 80 для локальной сети, а 81 нет (рис. [-@fig:012]).

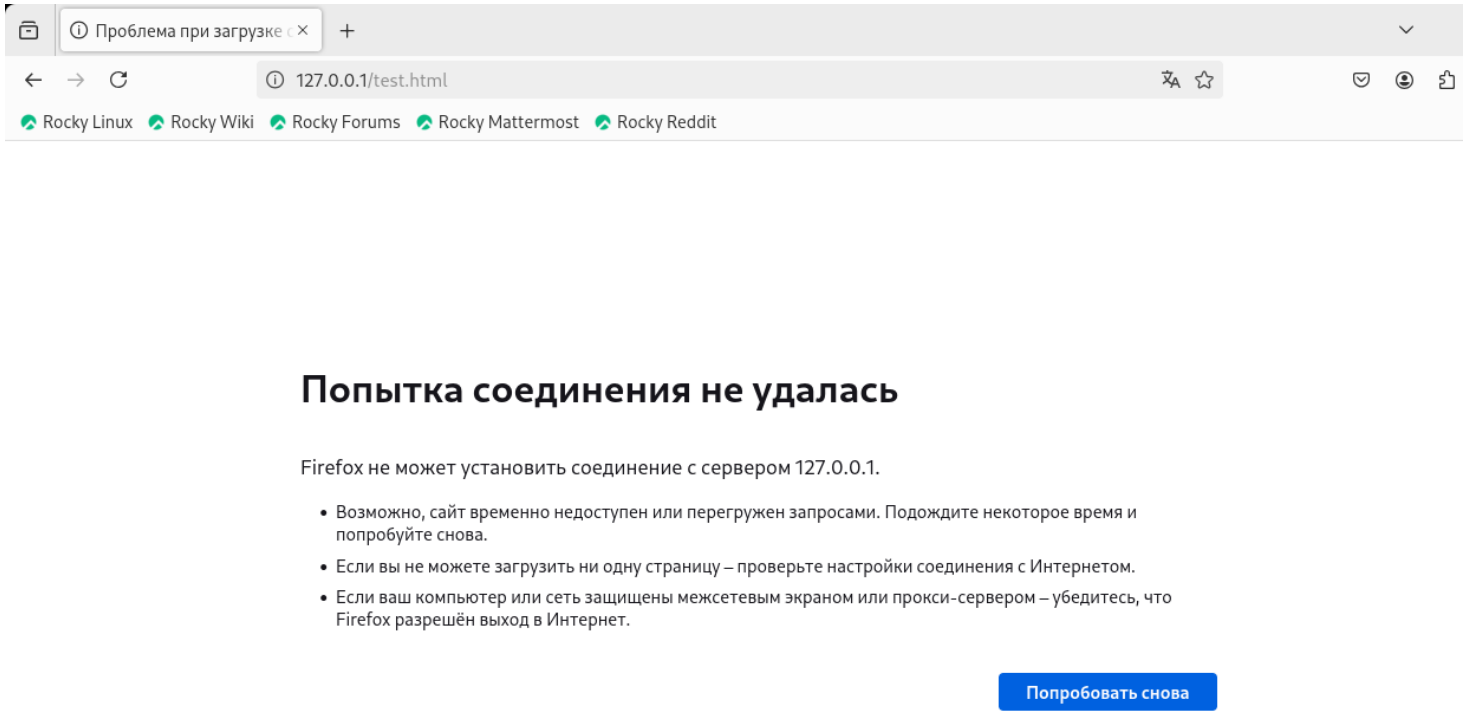

Рис.12. Попытка прослушивания другого порта

Просмотрела файл `/var/log/httpd/error_log.` Запись появилась в файле error_log (рис. [-@fig:013]).

```
[mgandrianova@localhost ~]$ sudo cat /var/log/httpd/error_log
[Wed Oct 09 21:10:50.967219 2024] [core:notice] [pid 2860:tid 2860] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Wed Oct 09 21:10:50.974793 2024] [suexec:notice] [pid 2860:tid 2860] 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
[Wed Oct 09 21:10:51.020701 2024] [lbmethod_heartbeat:notice] [pid 2860:tid 2860] AH02282: No slotmem from mod_heartmonitor
[Wed Oct 09 21:10:51.094759 2024] [mpm_event:notice] [pid 2860:tid 2860] AH00489: Apache/2.4.57 (Rocky Linux) configured -- resuming normal operations
[Wed Oct 09 21:10:51.094808 2024] [core:notice] [pid 2860:tid 2860] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Wed Oct 09 21:32:17.302191 2024] [core:error] [pid 2868:tid 2965] (13)Permission denied: [client 127.0.0.1:57404] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Wed Oct 09 21:40:10.382464 2024] [core:error] [pid 2868:tid 2987] (13)Permission denied: [client 127.0.0.1:53564] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Wed Oct 09 21:40:51.946583 2024] [core:error] [pid 2868:tid 2984] (13)Permission denied: [client 127.0.0.1:33096] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Wed Oct 09 21:41:12.888745 2024] [core:error] [pid 2868:tid 3016] (13)Permission denied: [client 127.0.0.1:43038] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Wed Oct 09 21:41:14.282998 2024] [core:error] [pid 2868:tid 3012] (13)Permission denied: [client 127.0.0.1:43038] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Wed Oct 09 21:42:33.873245 2024] [core:error] [pid 2868:tid 3018] (13)Permission denied: [client 127.0.0.1:52002] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Wed Oct 09 21:42:45.243468 2024] [core:error] [pid 2868:tid 3013] (13)Permission denied: [client 127.0.0.1:55880] AH00035: access to /test.html denied (files
ystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[mgandrianova@localhost ~]$
```

Рис.13. Проверка лог-файлов

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 (рис. [-@fig:014]).

```
[mgandrianova@localhost ~]$ sudo semanage port -a -t http_port_t -p tcp 81
Port tcp/81 already defined, modifying instead
[mgandrianova@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.14. Проверка портов

Перезапускаю сервер Apache (рис. [-@fig:015]).

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

Рис.15. Перезапуск сервера

Теперь он работает, ведь мы внесли порт 81 в список портов `http_port_t` (рис. [-@fig:016]).

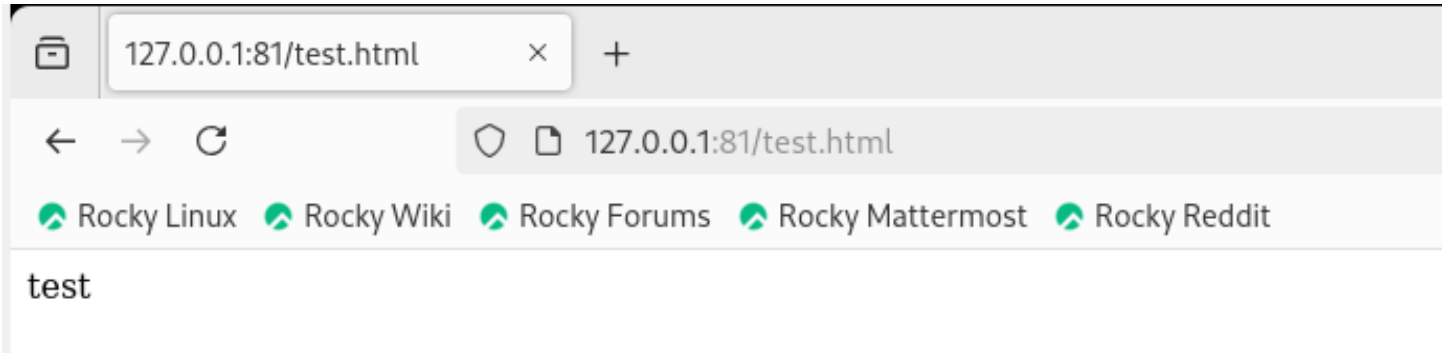

Рис.16. Проверка сервера

Возвращаю в файле /etc/httpd/httpd.conf порт 80, вместо 81. Проверяю, что порт 81 удален, это правда (рис. [-@fig:017]).

```
[mgandrianova@localhost ~]$ sudo nano /etc/httpd/conf/httpd.conf
[mgandrianova@localhost ~]$ sudo semanage port -d -t http_port_t -p tcp 81
[mgandrianova@localhost ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
```

Рис.17. Проверка порта 81

Далее удаляю файл test.html, проверяю, что он удален (рис. [-@fig:018]).

```
[mgandrianova@localhost ~]$ sudo rm /var/www/html/test.html
[mgandrianova@localhost ~]$ ls -lZ /var/www/html
итого 0
```

Рис.18. Удаление файла

Выводы

• 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.