# Отчет по лабораторной работе №6

**Мандатное разграничение прав в Linux**

Легиньких Галина Андреевна

# Содержание

# Список иллюстраций

# Список таблиц

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

**1.** Скачала httpd. (рис. 2.1)

```
[galeginkikh@galeginkikh ~]$ su
Password:
[root@galeginkikh galeginkikh]# yum install httpd
Last metadata expiration check: 1 day, 16:49:54 ago on Wed 18 Sep 2024 09:15:27 PM
 MSK.
Dependencies resolved.
================================================================================
 Package       Arch   Version                                  Repo       Size
================================================================================
Installing:
 httpd         x86_64 2.4.37-65.module+el8.10.0+1842+4a9649e8.2 appstream 1.4 M
Installing dependencies:
 apr           x86_64 1.6.3-12.el8                             appstream 128 k
 apr-util      x86_64 1.6.1-9.el8                              appstream 105 k
 httpd-filesystem
```

Рис. 2.1: install httpd

**2.** В конфигурационном файле /etc/httpd/httpd.conf задала параметр ServerName. Отключила пакетный фильтр. (рис. 2.2)

```
[root@galeginkikh galeginkikh]# cd /etc/httpd
[root@galeginkikh httpd]# echo "ServerName test.ru" >> httpd.conf
[root@galeginkikh httpd]# iptables -F
[root@galeginkikh httpd]# iptables -P INPUT ACCEPT iptables -P OUTPUT ACCEPT
Bad argument `iptables'
Try `iptables -h' or 'iptables --help' for more information.
[root@galeginkikh httpd]# iptables -P INPUT ACCEPT
[root@galeginkikh httpd]# iptables -P OUTPUT ACCEPT
[root@galeginkikh httpd]#
```

Рис. 2.2: Пакетные фильтры

**3.** Вошла в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted. (рис. 2.3)

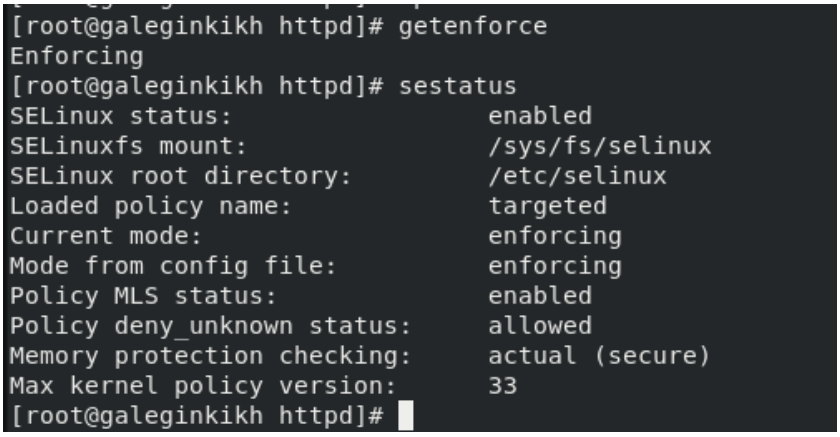


Рис. 2.3: SELinux

**4.** Обратитилась с помощью браузера к веб-серверу, запущенному на компьютере, и убедилась, что последний работает. Он не работает, запустила его так же, но с параметром start. (рис. 2.4) (рис. 2.5)

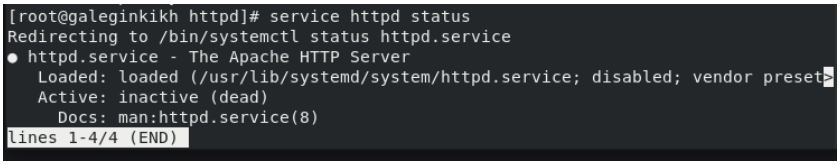


Рис. 2.4: Сервер_1

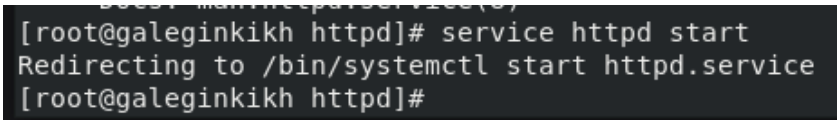


Рис. 2.5: Сервер_2

**5.** Нашла веб-сервер Apache в списке процессов, определила его контекст безопасности. (рис. 2.6)

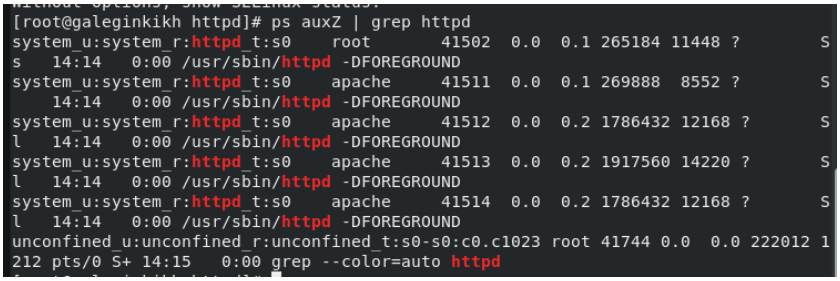


Рис. 2.6: Веб-сервер Apache

**6.** Посмотрела текущее состояние переключателей SELinux для Apache. Обратила внимание, что многие из них находятся в положении «off». (рис. 2.7)

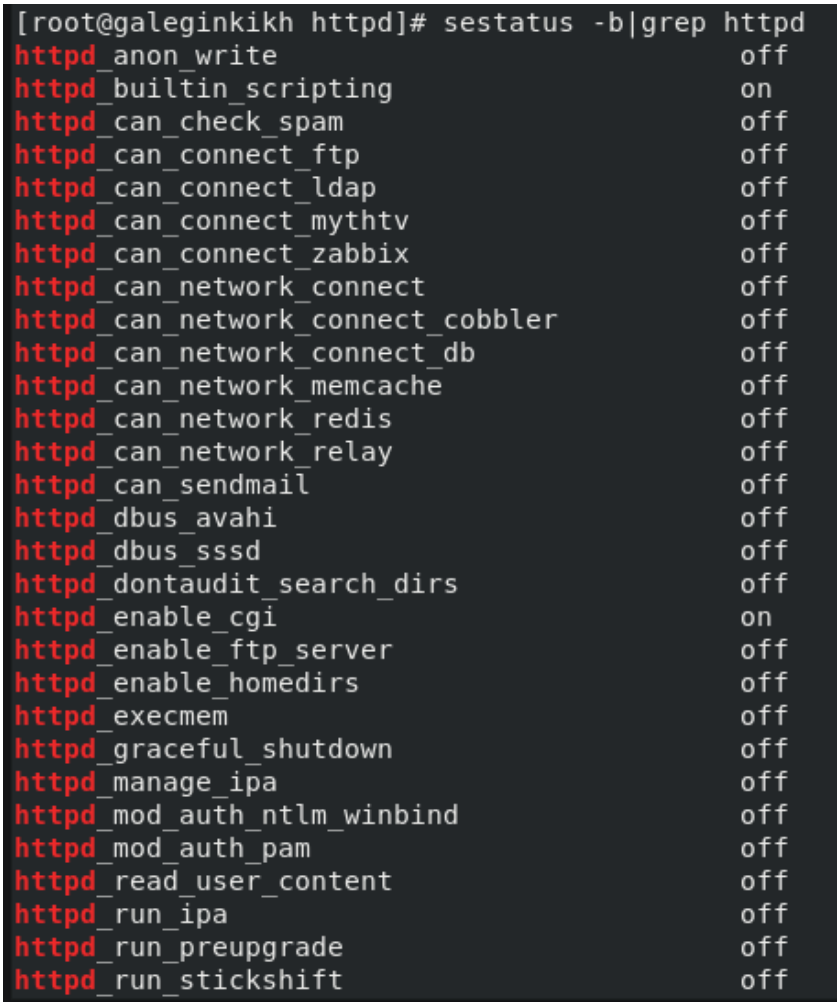


Рис. 2.7: Состояние переключателей SELinux

**7.** Посмотрела статистику по политике с помощью команды seinfo, также опре-

делила множество пользователей, ролей, типов. (рис. 2.8)

```
[root@galeginkikh httpd]# 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:            116272    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
  Auditallowxperm:       0    Dontauditxperm:        0
  Ibendportcon:          0    Ibpkeycon:             0
  Initial SIDs:         27    Fs_use:               34
  Genfscon:            107    Portcon:             649
  Netifcon:              0    Nodecon:               0
[root@galeginkikh httpd]#
```

Рис. 2.8: seinfo

**8.** Определила тип файлов и поддиректорий, находящихся в директории /var/www. (рис. 2.9)

```
[root@galeginkikh httpd]# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Aug 12 11:1
4 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 Aug 12 11:1
4 html
```

Рис. 2.9: Тип файлов и поддиректорий в /var/www

**9.** Определила тип файлов, находящихся в директории /var/www/html. (рис. 2.10)

```
[root@galeginkikh httpd]# ls -lZ /var/www/html
total 0
```

Рис. 2.10: Тип файлов и поддиректорий в /var/www/html

**10.** Определила круг пользователей, которым разрешено создание файлов в директории /var/www/html. (рис. 2.11)

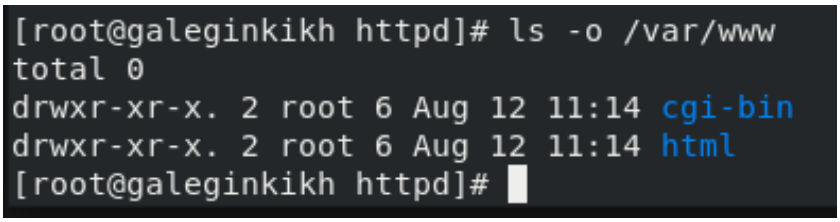


Рис. 2.11: Права на создание файлов

**11.** Создала от имени суперпользователя html-файл /var/www/html/test.html. (рис. 2.12)

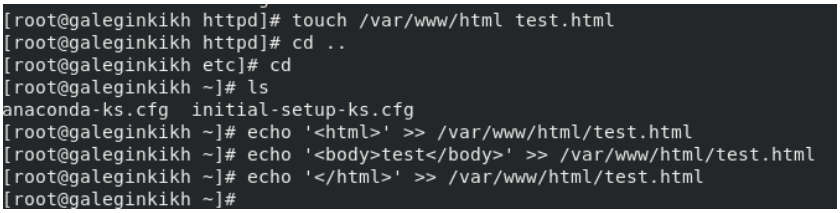


Рис. 2.12: test.html

**12.** Проверила контекст созданного файла. (рис. 2.13)


Рис. 2.13: Контекст test.html

**13.** Обратитилась к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. (рис. 2.14)

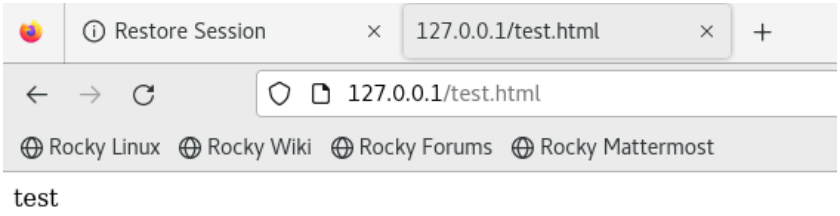


Рис. 2.14: Веб-сервер

**14.** Изучила справку man httpd_selinux и выяснила, какие контексты файлов определены для httpd. (рис. 2.15)

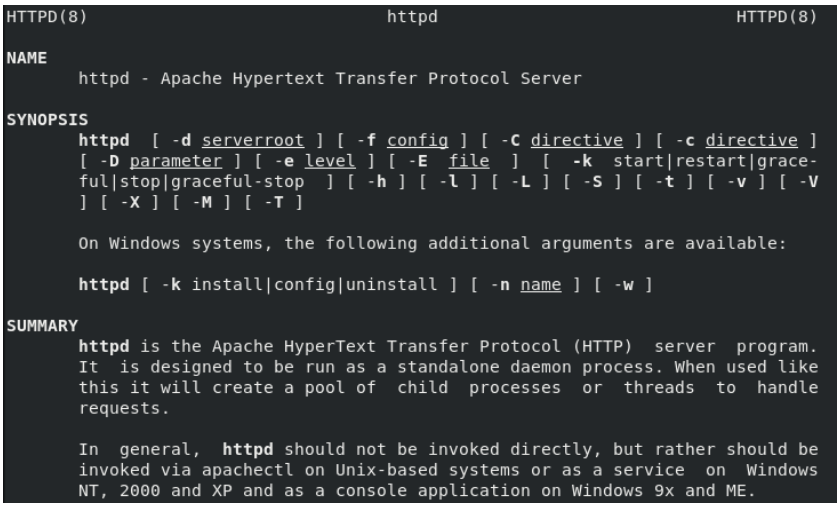


Рис. 2.15: man

**15.** Изменила контекст файла /var/www/html/test.html с httpd_sys_content_t на любой другой, к которому процесс httpd не должен иметь доступа. (рис. 2.16)

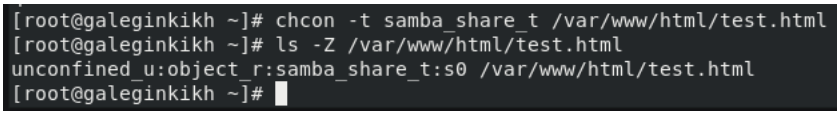


Рис. 2.16: Изменение контекста

**16.** Попробовала ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. (рис. 2.17)

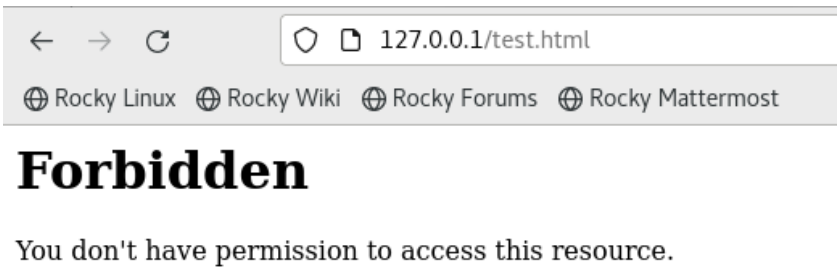


Рис. 2.17: Ошибка веб-сервера

**17.** Проанализировала ситуацию. Также просмотрела лог-файл. (рис. 2.18) (рис. 2.19)

```
[root@galeginkikh ~]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 Sep 20 14:26 /var/www/html/test.html
```

Рис. 2.18: Права

```
[root@galeginkikh ~]# tail /var/log/messages
Sep 20 14:33:19 galeginkikh dbus-daemon[799]: [system] Activating service name='or
g.fedoraproject.SetroubleshootPrivileged' requested by ':1.468' (uid=980 pid=43640
 comm="/usr/libexec/platform-python -Es /usr/sbin/setroub" label="system_u:system_
r:setroubleshootd_t:s0") (using servicehelper)
Sep 20 14:33:19 galeginkikh dbus-daemon[799]: [system] Successfully activated serv
ice 'org.fedoraproject.SetroubleshootPrivileged'
Sep 20 14:33:20 galeginkikh setroubleshoot[43640]: SELinux is preventing httpd fro
m getattr access on the file /var/www/html/test.html. For complete SELinux message
s run: sealert -l 0b5c2438-50ed-4f9a-9470-19169920a0b0
```

Рис. 2.19: Лог-файл

**18.** Нашла строчку Listen 80 и заменила её на Listen 81. (рис. 2.20)

```
#Listen 12.34.56.78:80
Listen 81
```

Рис. 2.20: Listen 81

**19.** Проанализировала лог-файлы. (рис. 2.21)

```
[root@galeginkikh ~]# tail -n1 /var/log/messages
Sep 20 14:44:44 galeginkikh systemd[1]: setroubleshootd.service: Succeeded.
```

Рис. 2.21: Лог-файлы_2

**20.** Проверила список портов командой. Убедитесь, что порт 81 появился в списке. (рис. 2.22)

```
[root@galeginkikh ~]# semanage port -a -t http_port_t -p tcp 81
usage: semanage [-h]
                {import,export,login,user,port,ibpkey,ibendport,interface,module,n
ode,fcontext,boolean,permissive,dontaudit}
                ...
semanage: error: unrecognized arguments: -p 81
[root@galeginkikh ~]# 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@galeginkikh ~]#
```

Рис. 2.22: Список портов

**21.** Попробовала запустить веб-сервер Apache ещё раз. (рис. 2.23)

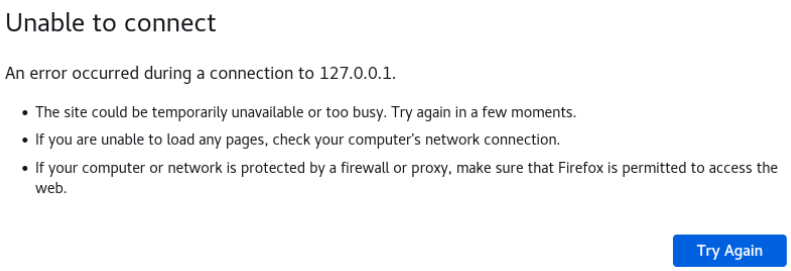


Рис. 2.23: Unable to connect

**22.** Вернула контекст httpd_sys_content__t к файлу /var/www/html/ test.html. После этого попробовала получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1:81/test.html. (рис. 2.24) (рис. 2.25)

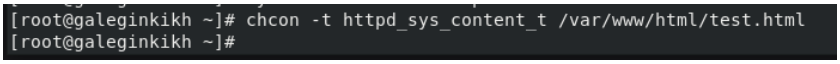


Рис. 2.24: chcon

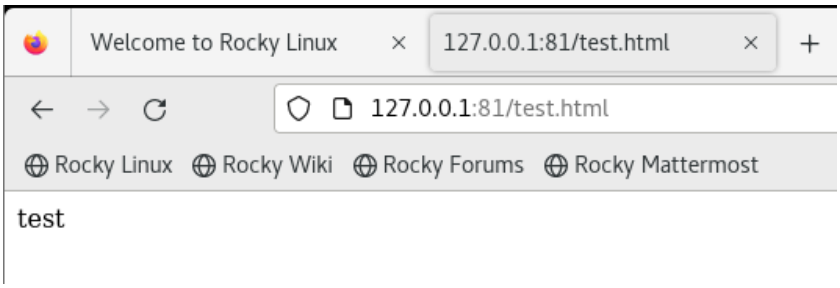


Рис. 2.25: Веб-сервер_81

**23.** Исправила обратно конфигурационный файл apache, вернув Listen 80.

**24.** Удалила привязку http_port_t к 81 порту и проверьте, что порт 81 удалён. (рис. 2.26)

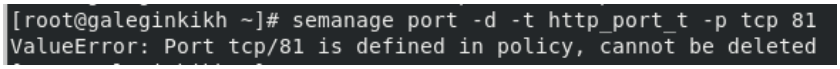


Рис. 2.26: Порт 81

24. Удалила файл /var/www/html/test.html. (рис. 2.27)

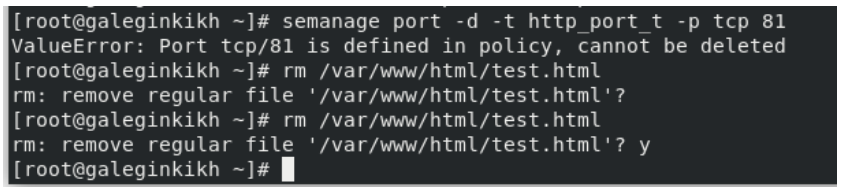


Рис. 2.27: rm tast.html

# 3 Вывод

Развила навыки администрирования ОС Linux. Получила первое практическое знакомство с технологией SELinux. Проверила работу SELinx на практике совместно с веб-сервером Apache.