

# Лабораторная работа #6

Мандатное разграничение прав в Linux.

Критский Сергей Димитриевич

# Содержание

Цель работы	3
Выполнение лабораторной работы	4
Начало работы . . . . .	4
Создание веб-страницы . . . . .	7
Изменение конфигурации сервера и страницы . . . . .	9
Выводы	12

## 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

## Начало работы

Запустил сервер, проверил корректность запуска Apache и состояние переключателей SELinux.

```
[sdkritskiy@SDKritskiy ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[sdkritskiy@SDKritskiy ~]$ 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; vendor pr>
   Active: active (running) since Sat 2022-10-15 14:24:01 MSK; 3s ago
     Docs: man:httpd.service(8)
  Main PID: 40421 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 12213)
    Memory: 50.6M
       CPU: 181ms
    CGroup: /system.slice/httpd.service
           └─40421 /usr/sbin/httpd -DFOREGROUND
             └─40429 /usr/sbin/httpd -DFOREGROUND
               └─40432 /usr/sbin/httpd -DFOREGROUND
                 └─40434 /usr/sbin/httpd -DFOREGROUND
                   └─40437 /usr/sbin/httpd -DFOREGROUND

Oct 15 14:24:00 SDKritskiy.localdomain systemd[1]: Starting The Apache HTTP Ser>
Oct 15 14:24:01 SDKritskiy.localdomain systemd[1]: Started The Apache HTTP Serv>
Oct 15 14:24:01 SDKritskiy.localdomain httpd[40421]: Server configured, listeni>
```

Рис. 1: Запуск сервера

```

[SDKritskiy@SDKritskiy ~]$ ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 SDKrits+ 40368 0.0 0.4 23
5988 9232 pts/0 T 14:23 0:00 /bin/systemctl status httpd.service
system_u:system_r:httpd_t:s0 root 40421 0.3 0.5 20064 11620 ?
Ss 14:24 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 40429 0.0 0.3 21516 7316 ?
S 14:24 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 40432 0.0 1.0 1210352 21372 ?
Sl 14:24 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 40434 0.0 1.0 1079216 21368 ?
Sl 14:24 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 40437 0.0 1.0 1079216 21368 ?
Sl 14:24 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 SDKrits+ 40664 0.0 0.4 23
5988 9132 pts/0 T 14:24 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 SDKrits+ 40683 0.0 0.1 22
1668 2284 pts/0 S+ 14:24 0:00 grep --color=auto httpd
[SDKritskiy@SDKritskiy ~]$ sestatus -bigrep httpd
sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]

-v Verbose check of process and file contexts.

```

Рис. 2: Поиск Apache

```
[sdkritskiy@SDKritskiy ~]$ 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_manage_courier_spool 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_relay off
httpd_can_sendmail off
httpd_dbus_avahi off
httpd_dbus_sssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execmem off
httpd_graceful_shutdown off
httpd_manage_ipa off
```

Рис. 3: КСостояние переключателей SELinux

Просмотрел статистику по политике

```

[sdkritskiy@SDKritskiy ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 133      Permissions:             454
Sensitivities:           1        Categories:             1024
Types:                   5002     Attributes:              254
Users:                   8         Roles:                  14
Booleans:                347      Cond. Expr.:           381
Allow:                   63996     Neverallow:             0
Auditallow:              168      Dontaudit:              8417
Type_trans:              258486    Type_change:            87
Type_member:              35       Range_trans:            5960
Role_allow:              38       Role_trans:             420
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:                 33
Genfscon:                106      Portcon:                651

```

Рис. 4: Статистика по политике

## Создание веб-страницы

Создал простую Web-страницу с надписью test. Проверил ее контекст и открыл ее.

```

[sdkritskiy@SDKritskiy ~]$ vi /var/www/html/test.html
[sdkritskiy@SDKritskiy ~]$ ls -lZ /var/www/html
total 4
-rwxrwxrwx. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 Oct 4:29 test.html
[sdkritskiy@SDKritskiy ~]$ ls -Z /var/www/html/test.html

```

Рис. 5: Контекст файла с веб-страницей

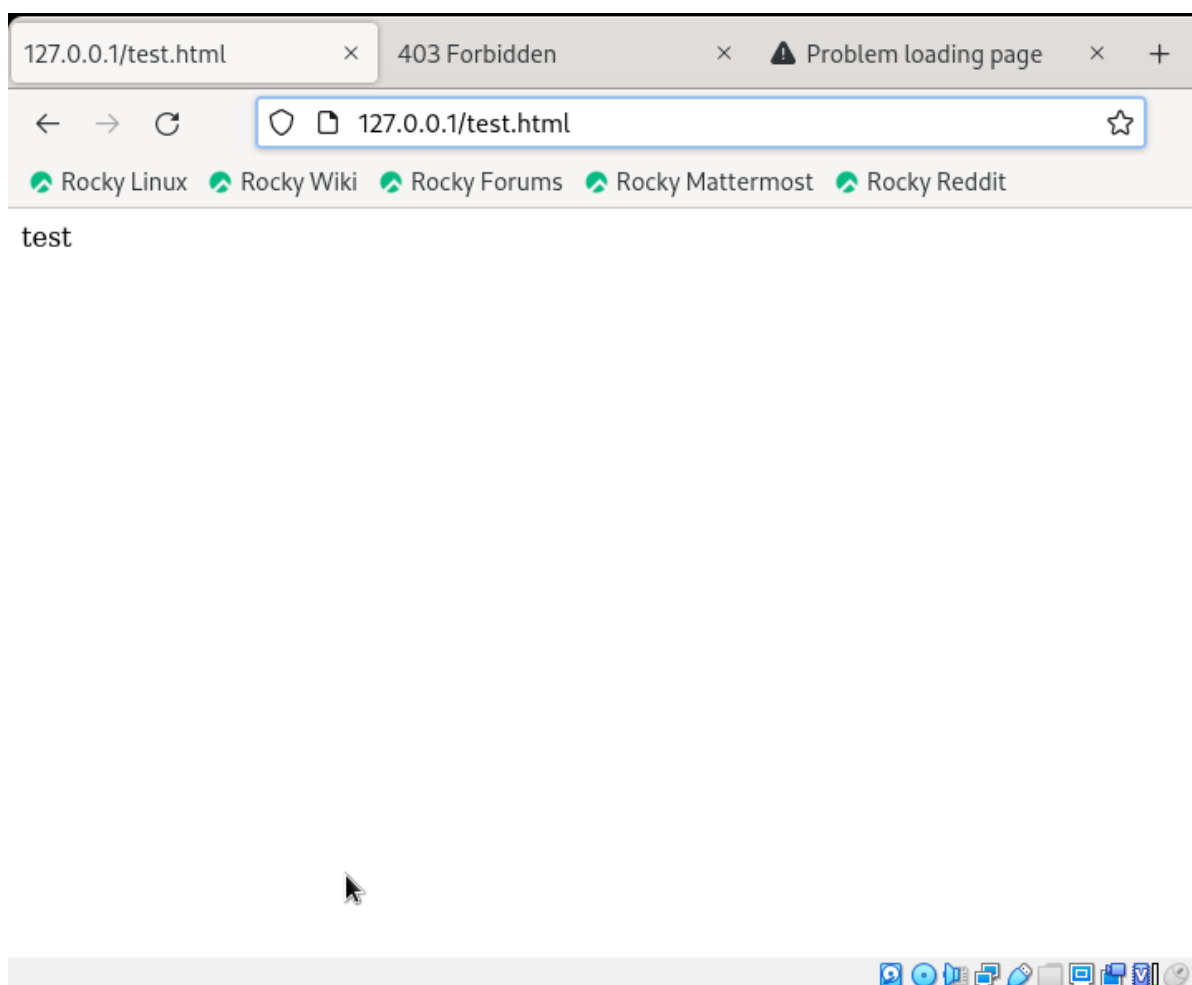


Рис. 6: Сама веб-страница

Изменил контекст Web-страницы и снова попытался ее открыть.

```
ject_r:samba_share_t:s0 : operation not permitted
[sdkritskiy@SDKritskiy ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[sdkritskiy@SDKritskiy ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[sdkritskiy@SDKritskiy ~]$ tail /var/log/messages
```

Рис. 7: Изменение контекста



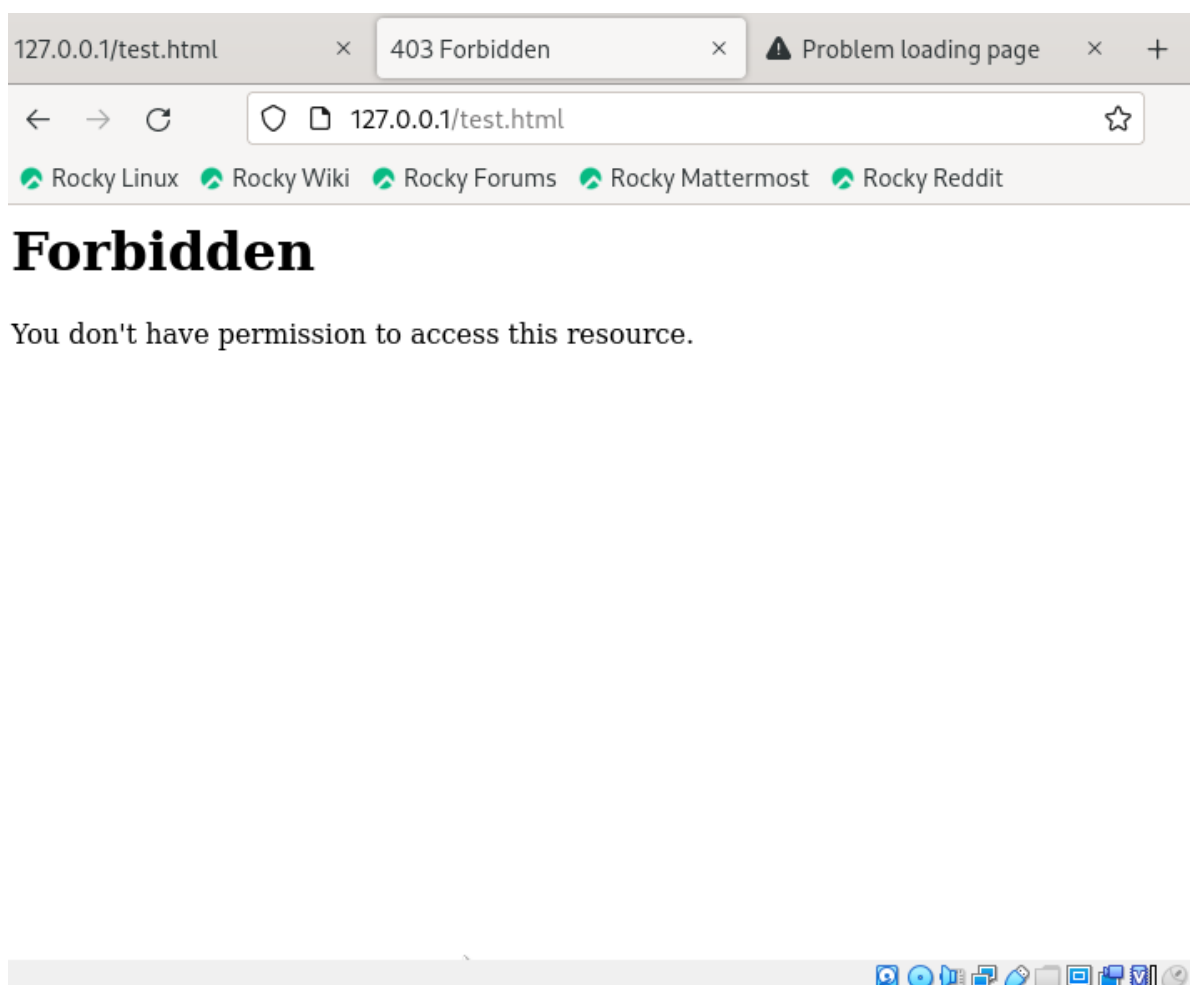
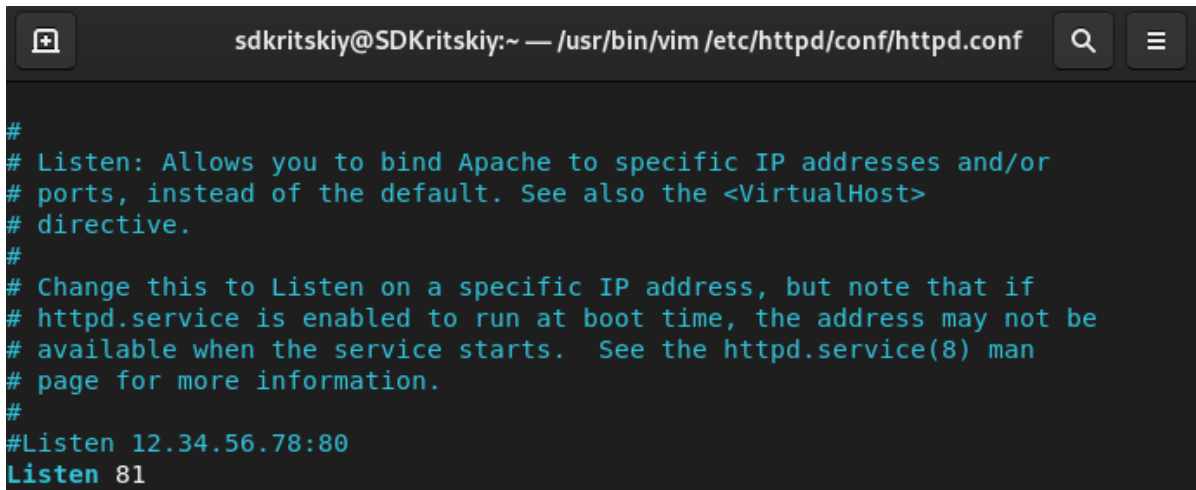


Рис. 8: Веб-страница

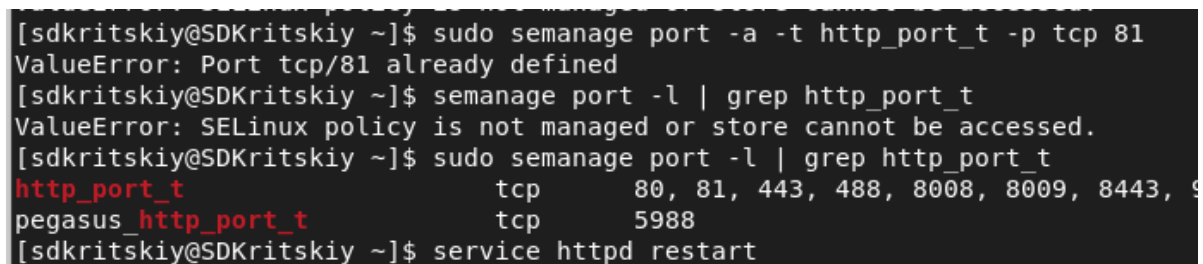
## Изменение конфигурации сервера и страницы

Поставил прослушивание 81-го порта, указал его в файле и добавил его в список портов. Успешно открыл Web-страницу с изначальным контекстом.



```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# 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
```

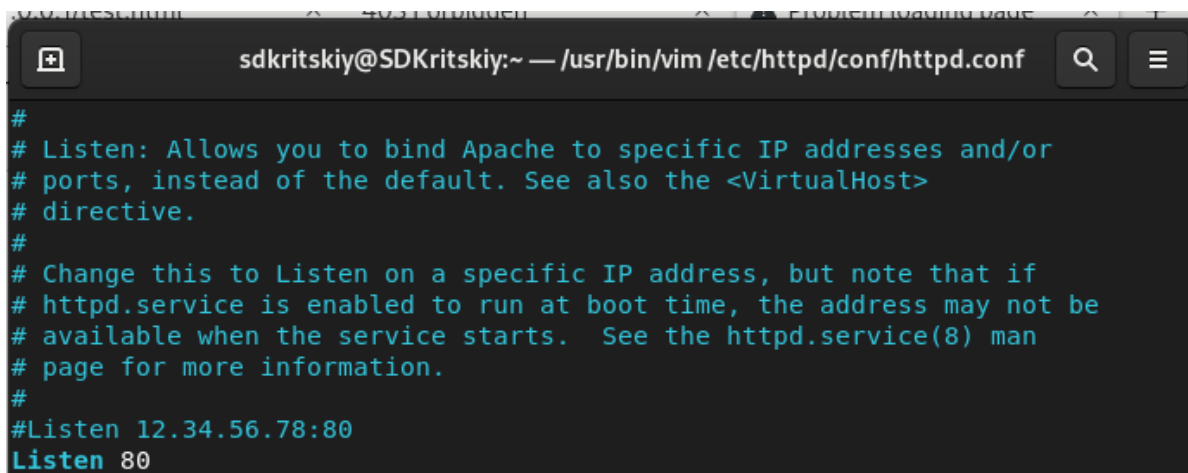
Рис. 9: Указание 81 порта



```
[sdkritskiy@SDKritskiy ~]$ sudo semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[sdkritskiy@SDKritskiy ~]$ semanage port -l | grep http_port_t
ValueError: SELinux policy is not managed or store cannot be accessed.
[sdkritskiy@SDKritskiy ~]$ sudo 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
[sdkritskiy@SDKritskiy ~]$ service httpd restart
```

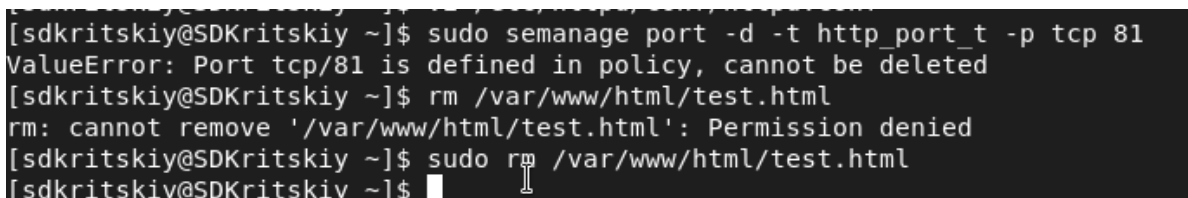
Рис. 10: Прослушивание 81 порта

Вернул все настройки по-умолчанию и удалил файл Web-страницы.



```
sdkritskiy@SDKritskiy:~ — /usr/bin/vim /etc/httpd/conf/httpd.conf
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# 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 80
```

Рис. 11: Указание 80 порта



```
[sdkritskiy@SDKritskiy ~]$ sudo semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[sdkritskiy@SDKritskiy ~]$ rm /var/www/html/test.html
rm: cannot remove '/var/www/html/test.html': Permission denied
[sdkritskiy@SDKritskiy ~]$ sudo rm /var/www/html/test.html
[sdkritskiy@SDKritskiy ~]$
```

Рис. 12: Удаление страницы и 81 порта

## Выводы

Я развил навыки администрирования ОС Linux, получил первое практическое знакомство с технологией SELinux и проверил работу SELinux на практике совместно с веб-сервером Apache.