

Лабораторная работа №6

Жукова Виктория

RUDN University, 15 October 2022 Moscow, Russia

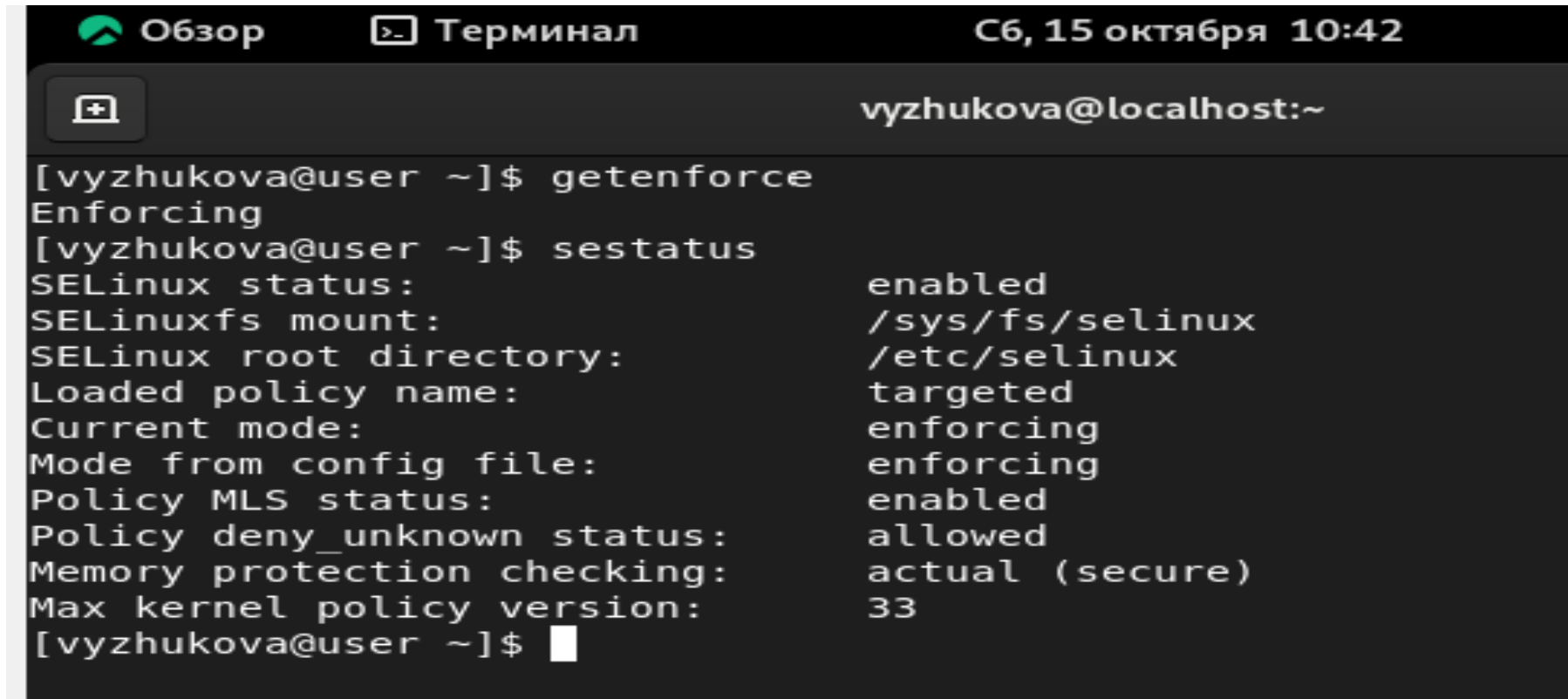
Мандатное разграничение прав в Linux

Цель выполнения 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

Выполнение работы



The image shows a terminal window with a dark background. At the top, there is a title bar with three tabs: 'Обзор' (Overview) with a green icon, 'Терминал' (Terminal) with a terminal icon, and a timestamp 'Сб, 15 октября 10:42'. Below the tabs, the terminal title is 'vyzhukova@localhost:~'. The terminal content shows the user 'vyzhukova' at the prompt '[vyzhukova@user ~]\$' running the command 'getenforce', which returns 'Enforcing'. Then, the user runs 'sestatus', which displays the following SELinux status information:

```
[vyzhukova@user ~]$ getenforce
Enforcing
[vyzhukova@user ~]$ 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
[vyzhukova@user ~]$
```

Рис.1 Режим и политика SELinux

Выполнение работы

```
Redirecting to /bin/systemctl start httpd.service
[root@user ~]# 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 11:54:16 MSK; 8s ago
     Docs: man:httpd.service(8)
  Main PID: 108160 (httpd)
    Status: "Started, listening on: port 80"
     Tasks: 213 (limit: 12210)
   Memory: 15.0M
      CPU: 38ms
   CGroup: /system.slice/httpd.service
           └─108160 /usr/sbin/httpd -DFOREGROUND
             └─108161 /usr/sbin/httpd -DFOREGROUND
               └─108162 /usr/sbin/httpd -DFOREGROUND
                 └─108163 /usr/sbin/httpd -DFOREGROUND
                   └─108164 /usr/sbin/httpd -DFOREGROUND

окт 15 11:54:15 user.localhost systemd[1]: Starting The Apache HTTP Server...
окт 15 11:54:16 user.localhost httpd[108160]: AH00558: httpd: Could not reliabl>
окт 15 11:54:16 user.localhost systemd[1]: Started The Apache HTTP Server.
окт 15 11:54:16 user.localhost httpd[108160]: Server configured, listening on: >
lines 1-20/20 (END)
```

Рис.2 Запуск Apache web server

Выполнение работы

```
OK: 15 11:54:10 user@localhost: httpd[108160]: server configured, listening on:
[root@user ~]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root      108160  0.0  0.5  20092 11508 ?
Ss   11:54   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    108161  0.0  0.3   21416   7244 ?
S    11:54   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    108162  0.0  0.4 1079216   8816 ?
Sl   11:54   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    108163  0.0  0.4 1079216   8816 ?
Sl   11:54   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache    108164  0.0  0.4 1210352   8816 ?
Sl   11:54   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 108384 0.0  0.1  22169
2 2436 pts/0 S+ 11:55   0:00 grep --color=auto httpd
[root@user ~]#
```

Рис.3 Контекст безопасности Apache web server

Выполнение работы

```
Without options, show SELinux status.  
[root@user ~]# sestatus -b | grep httpd  
httpd_anon_write off  
httpd_builtin_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
```

Рис.4 Текущее состояние переключателей SELinux для Apache

Выполнение работы

```
[root@user ~]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version: 33 (MLS enabled)
Target Policy: selinux
Handle unknown classes: allow
Classes: 133
Sensitivities: 1
Types: 5002
Users: 8
Booleans: 347
Allow: 63996
Auditallow: 168
Type_trans: 258486
Type_member: 35
Role_allow: 38
Constraints: 72
MLS_Constrain: 72
Permissives: 0
Defaults: 7
Allowxperm: 0
Auditallowxperm: 0
Ibendportcon: 0
Initial SIDs: 27
Permissions: 454
Categories: 1024
Attributes: 254
Roles: 14
Cond. Expr.: 381
Neverallow: 0
Dontaudit: 8417
Type_change: 87
Range_trans: 5960
Role_trans: 420
Validatetrans: 0
MLS_Val. Tran: 0
Polcap: 5
Typebounds: 0
Neverallowxperm: 0
Dontauditxperm: 0
Ibpkeycon: 0
Fs_use: 33
```

Рис.5 Тип файлов и поддиректорий

Выполнение работы

```
[root@user ~]# cd /var/www/html
[root@user html]# touch test.html
[root@user html]# nono test.html
bash: nono: command not found...
[root@user html]# vim test.html
[root@user html]# cat test.html
<html>
<body>test</body>
</html>
[root@user html]#
```

Рис.6 Создание файла test.html

Выполнение работы

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

Текст файла test.html

Выполнение работы

```
7/11/2016  
[root@user html]# ps auxZ | grep test.html  
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 108689 0.0 0.1 22182  
8 2380 pts/0 S+ 12:09 0:00 grep --color=auto test.html  
[root@user html]#
```

Рис.7 Контекст файла test.html

Выполнение работы

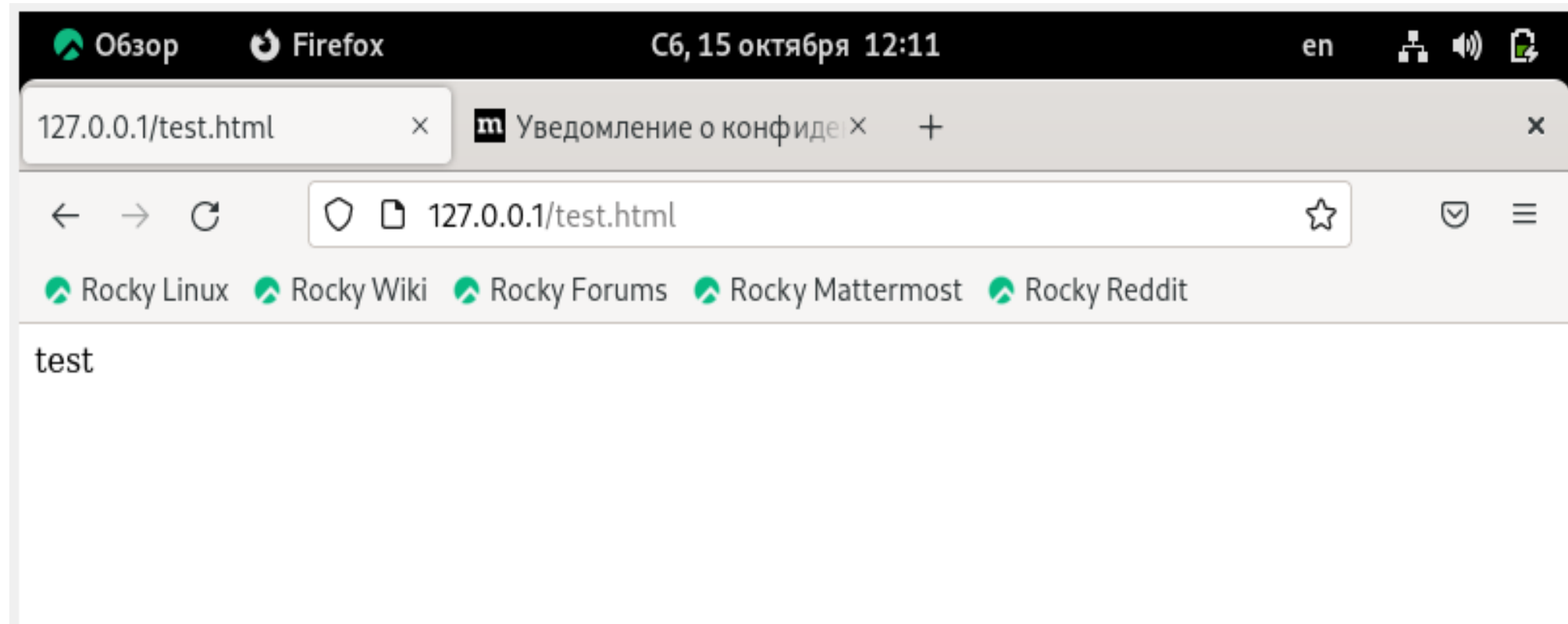


Рис.8 Веб страница

Выполнение работы

```
[root@user html]# chcon -t samba_share_t /var/www/html/test.html  
[root@user html]# ls -Z /var/www/html/test.html  
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html  
[root@user html]#
```

Рис.10 Изменения контекста файла test.html

Выполнение работы

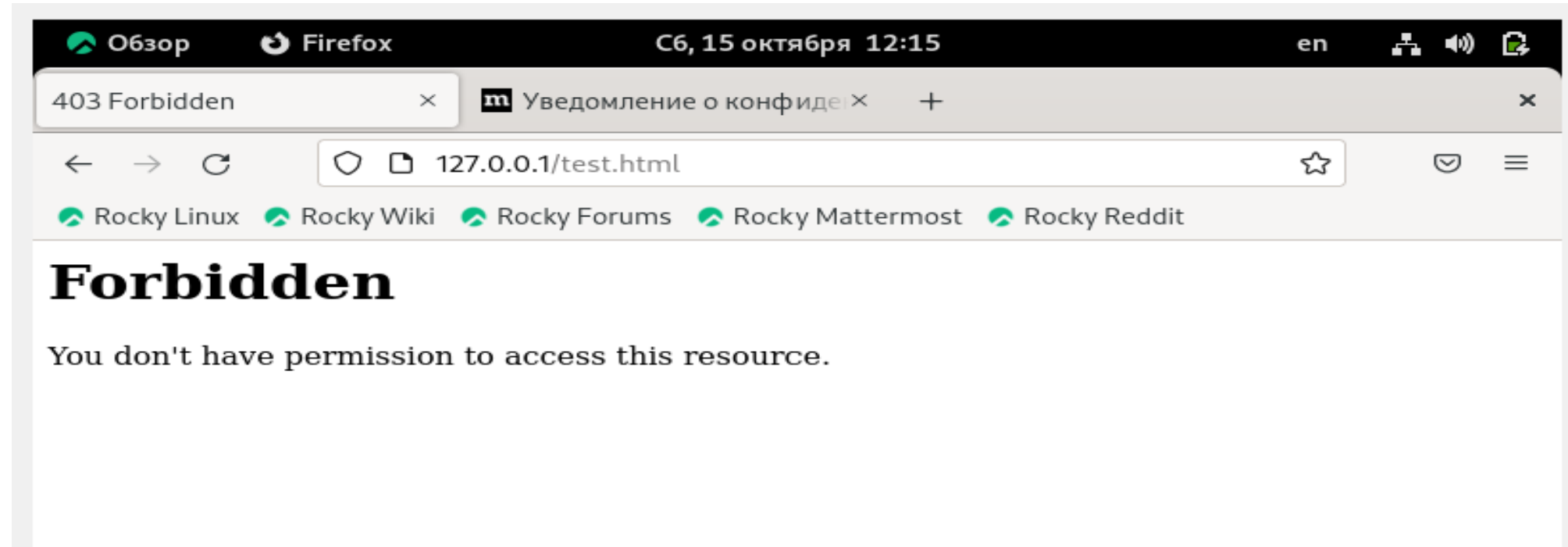


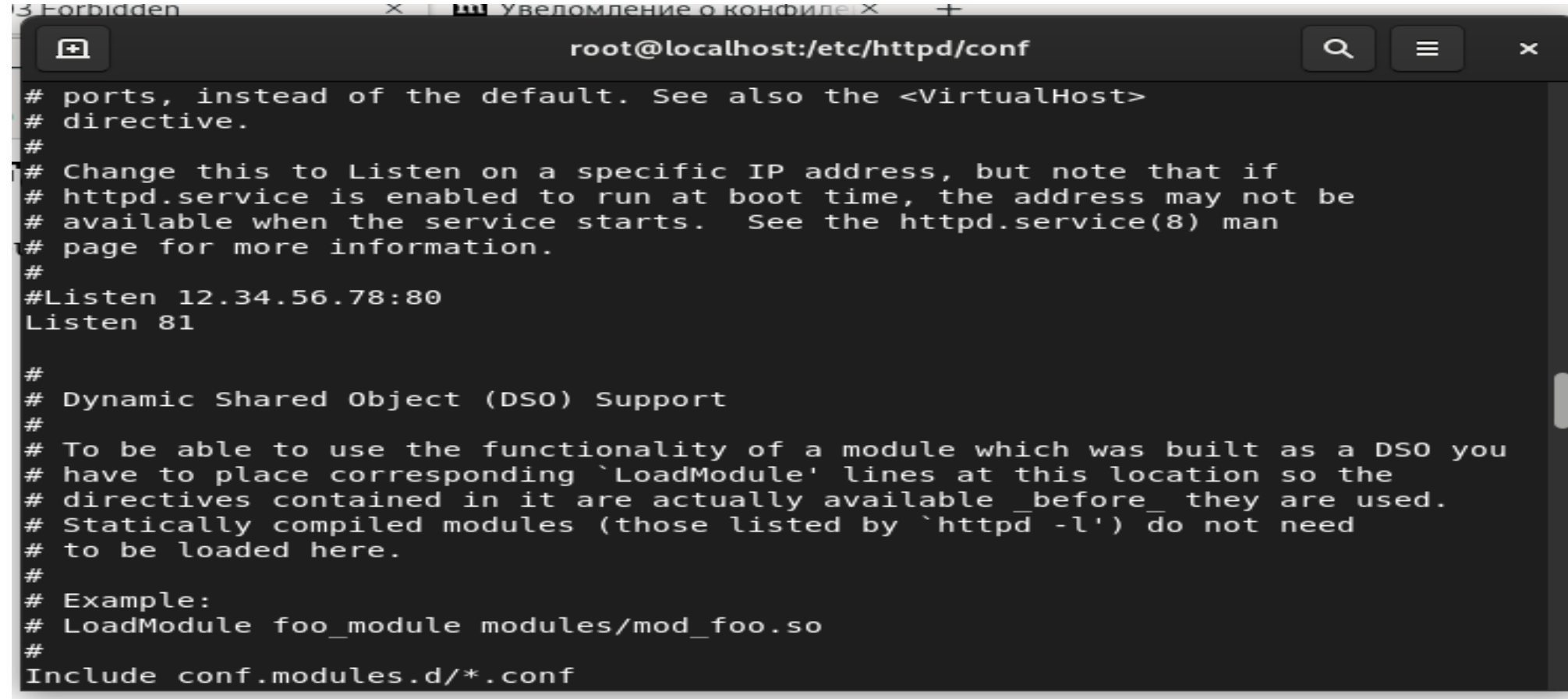
Рис.11 Доступ к странице запрещен

Выполнение работы

```
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@user_html]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 окт 15 12:07 /var/www/html/test.html
[root@user_html]# tail /var/log/messages
Oct 15 12:15:46 user systemd[1]: Started dbus-:1.10-org.fedoraproject.Setroubles
hootPrivileged@0.service.
Oct 15 12:15:47 user setroubleshoot[109065]: SELinux запрещает /usr/sbin/httpd д
оступ getattr к файл /var/www/html/test.html. Для выполнения всех сообщений SELi
nux: sealert -l dd1386df-4eaf-4542-ace0-ebb89bbbed0e2
Oct 15 12:15:47 user setroubleshoot[109065]: SELinux запрещает /usr/sbin/httpd д
оступ getattr к файл /var/www/html/test.html.#012#012***** Модуль restorecon пр
едлагает (точность 92.2) *****#012#012Если вы хотите исправ
ить метку.$TARGETЗнак _PATH по умолчанию должен быть httpd_sys_content_t#012То в
ы можете запустить restorecon. Возможно, попытка доступа была остановлена из-за
недостаточных разрешений для доступа к родительскому каталогу, и в этом случае п
опытайтесь соответствующим образом изменить следующую команду.#012Сделать#012# /
sbin/restorecon -v /var/www/html/test.html#012#012***** Модуль public_content п
редлагает (точность 7.83) *****#012#012Если вы хотите лечить te
st.html как общедоступный контент#012То необходимо изменить метку test.html с pu
blic_content_t на public_content_rw_t.#012Сделать#012# semanage fcontext -a -t p
ublic_content_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test
.html'#012#012***** Модуль catchall предлагает (точность 1.41) *****
*****#012#012Если вы считаете, что httpd должно быть разрешено getattr до
```

Рис.12 Логи веб сервера

Выполнение работы



```
root@localhost:/etc/httpd/conf
# 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

#
# 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
```

Рис.14 Смена порта

Выполнение работы



Рис.15 Запуск на 81 порту

Выполнение работы



Рис.16 Установка порта

Выполнение работы



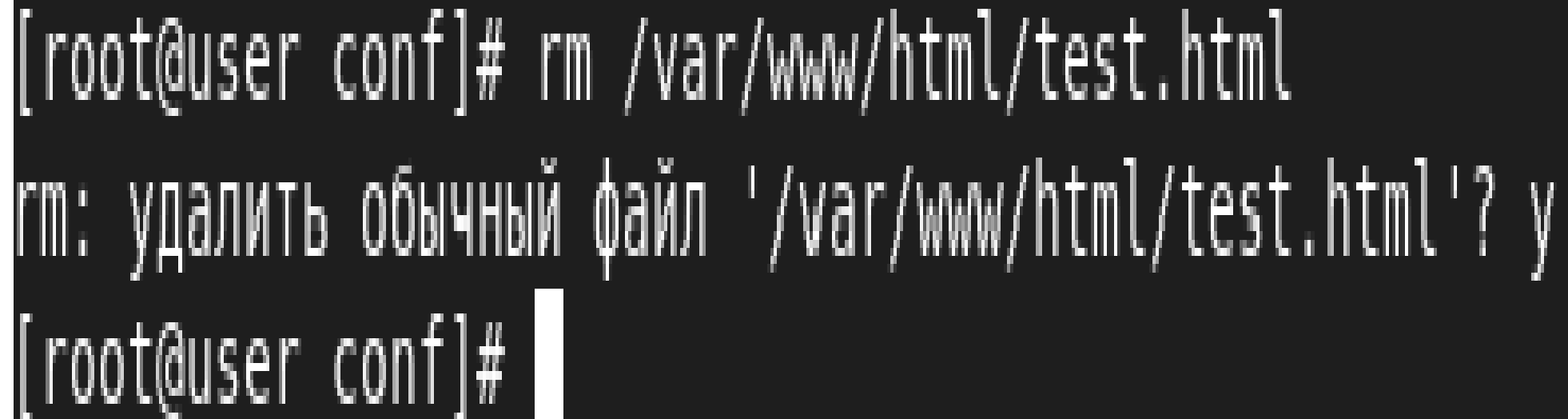
Рис.17 Работа веб сервера на 81 порту

Выполнение работы



Рис.18 Возвращение к 80 порту

Выполнение работы

A terminal window with a black background and white text. The prompt is [root@user conf]#. The command rm /var/www/html/test.html is entered. The output is rm: удалить обычный файл '/var/www/html/test.html'? y. The prompt [root@user conf]# is shown again with a white cursor bar.

```
[root@user conf]# rm /var/www/html/test.html  
rm: удалить обычный файл '/var/www/html/test.html'? y  
[root@user conf]#
```

Рис.19 Удаление файла страницы

Выводы

В ходе выполнения данной лабораторной работы я:

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

Спасибо за внимание!