

Отчёт по лабораторной работе №6

Информационная безопасность

Мандатное разграничение прав в Linux

Выполнила: Коняева Марина Александровна,
НФИбд-01-21, 1032217044

Содержание

Теоретическое введение	4
Цель работы	5
Выполнение лабораторной работы	6
Подготовка лабораторного стенда	6
Основная часть	7
Вывод	15
Список литературы. Библиография	16

Список иллюстраций

1	Установка httpd	6
2	Задача параметра ServerName	7
3	Отключение фильтров	7
4	Режим работы SELinux	7
5	Проверка работы сервера	7
6	Запуск сервера	8
7	Определение контекста безопасности	8
8	Текущее состояние переключателей SELinux для Apache	9
9	Статистика по политике	9
10	Тип файлов и поддиректорий в /var/www	10
11	Тип файлов и поддиректорий в /var/www/html	10
12	Создание test.html	10
13	Обращение к файлу через браузер	10
14	Смена контекста test.html	11
15	Обращение к файлу через браузер после смены контекста	11
16	Просмотр системного лог-файла	12
17	Изменение прослушивания TCP-порта	12
18	Перезапуск Apache	13
19	Добавление порта 81	13
20	Перезапуск Apache, возвращение изначального контекста test.html	13
21	Обращение к файлу через браузер после возвращения контекста	13
22	Возвращение порта 80 в httpd.conf	14
23	Работа команды удаления порта 81 и удаление test.html	14

Теоретическое введение

SELinux (англ. Security-Enhanced Linux — Linux с улучшенной безопасностью) — реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа. [2]

Apache HTTP-сервер — свободный веб-сервер. Apache является кроссплатформенным ПО, поддерживает операционные системы Linux, BSD, macOS, Microsoft Windows, Novell NetWare, BeOS.

Основными достоинствами Apache считаются надёжность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и т. д. Поддерживает IPv4. [3]

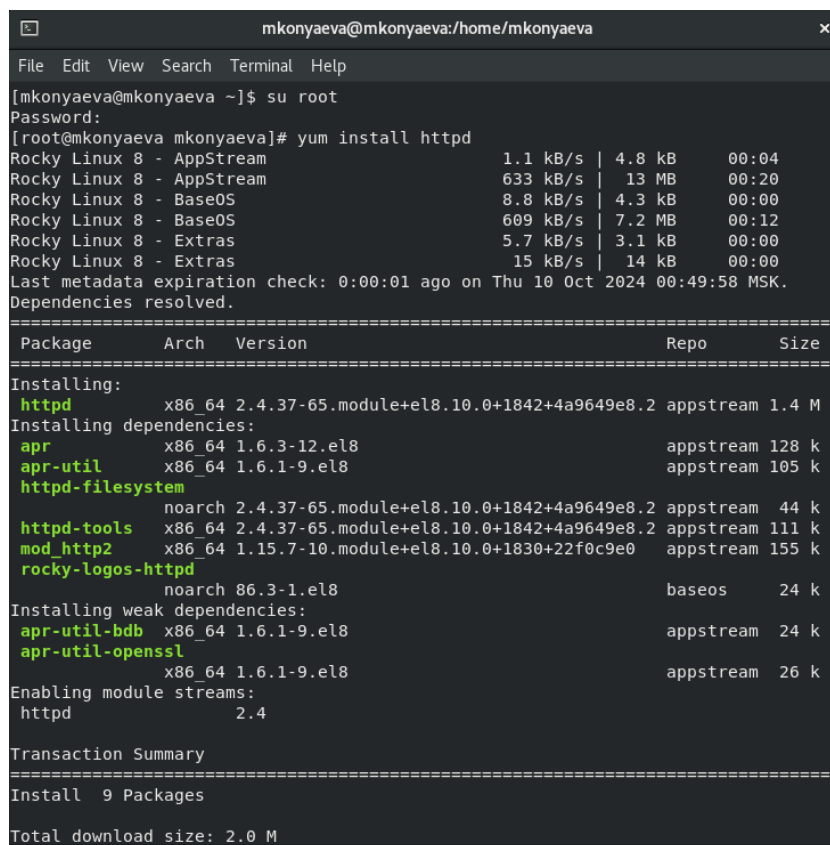
Цель работы

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

Подготовка лабораторного стенда

1. Установили httpd. (@fig:001)



```
mkonyaeva@mkonyaeva:/home/mkonyaeva
File Edit View Search Terminal Help

[mkonyaeva@mkonyaeva ~]$ su root
Password:
[root@mkonyaeva mkonyaeva]# yum install httpd
Rocky Linux 8 - AppStream 1.1 kB/s | 4.8 kB 00:04
Rocky Linux 8 - AppStream 633 kB/s | 13 MB 00:20
Rocky Linux 8 - BaseOS 8.8 kB/s | 4.3 kB 00:00
Rocky Linux 8 - BaseOS 609 kB/s | 7.2 MB 00:12
Rocky Linux 8 - Extras 5.7 kB/s | 3.1 kB 00:00
Rocky Linux 8 - Extras 15 kB/s | 14 kB 00:00
Last metadata expiration check: 0:00:01 ago on Thu 10 Oct 2024 00:49:58 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 noarch 2.4.37-65.module+el8.10.0+1842+4a9649e8.2 appstream 44 k
httpd-tools x86_64 2.4.37-65.module+el8.10.0+1842+4a9649e8.2 appstream 111 k
mod_http2 x86_64 1.15.7-10.module+el8.10.0+1830+22f0c9e0 appstream 155 k
rocky-logos-httpd noarch 86.3-1.el8 baseos 24 k
Installing weak dependencies:
apr-util-bdb x86_64 1.6.1-9.el8 appstream 24 k
apr-util-openssl x86_64 1.6.1-9.el8 appstream 26 k
Enabling module streams:
httpd 2.4

Transaction Summary
=====
Install 9 Packages
Total download size: 2.0 M
```

Рис. 1: Установка httpd

2. В конфигурационном файле `/etc/httpd/httpd.conf` необходимо задать параметр `ServerName`. (@fig:002)

```
[root@mkonyaeva mkonyaeva]# cd /etc/httpd
[root@mkonyaeva httpd]# echo "ServerName test.ru" >> httpd.conf
[root@mkonyaeva httpd]#
```

Рис. 2: Задача параметра ServerName

3. Отключили фильтры. (@fig:003)

```
[root@mkonyaeva httpd]# iptables -F
[root@mkonyaeva httpd]# iptables -P INPUT ACCEPT
[root@mkonyaeva httpd]# iptables -P OUTPUT ACCEPT
```

Рис. 3: Отключение фильтров

Основная часть

1. Убедились, что SELinux работает в режиме enforcing политики targeted. (@fig:004)

```
[root@mkonyaeva httpd]# getenforce
Enforcing
[root@mkonyaeva httpd]# 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
[root@mkonyaeva httpd]#
```

Рис. 4: Режим работы SELinux

2. Увидели, что сервер не работает и запустили его. (@fig:005, @fig:006)

```
[root@mkonyaeva httpd]# 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 preset: enabled)
   Active: inactive (dead)
     Docs: man:httpd.service(8)
```

Рис. 5: Проверка работы сервера

```

[root@mkonyaeva httpd]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@mkonyaeva httpd]# 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 preset: enabled)
   Active: active (running) since Thu 2024-10-10 00:57:11 MSK; 8s ago
     Docs: man:httpd.service(8)
  Main PID: 41302 (httpd)
    Status: "Started, listening on: port 80"
    Tasks: 213 (limit: 12248)
   Memory: 20.0M
   CGroup: /system.slice/httpd.service
           └─41302 /usr/sbin/httpd -DFOREGROUND
             └─41309 /usr/sbin/httpd -DFOREGROUND
               └─41310 /usr/sbin/httpd -DFOREGROUND
                 └─41311 /usr/sbin/httpd -DFOREGROUND
                   └─41312 /usr/sbin/httpd -DFOREGROUND

Oct 10 00:57:10 mkonyaeva.localdomain systemd[1]: Starting The Apache HTTP Server: listening on port 80...
Oct 10 00:57:11 mkonyaeva.localdomain systemd[1]: Started The Apache HTTP Server: listening on port 80...
Oct 10 00:57:11 mkonyaeva.localdomain httpd[41302]: Server configured, listening on: port 80

```

Рис. 6: Запуск сервера

3. Определили контекст безопасности Apache - `unconfined_u:unconfined_r:unconfined_t`. (@fig:007)

```

[root@mkonyaeva httpd]# ps auxZ | grep httpd
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 41197 0.0 0.3 292064
7104 pts/0 T 00:55 0:00 /bin/systemctl status httpd.service
system_u:system_r:httpd_t:s0 root 41302 0.0 0.5 265184 10940 ?
Ss 00:57 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41309 0.0 0.3 269888 7984 ?
S 00:57 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41310 0.0 0.4 1327680 9752 ?
Sl 00:57 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41311 0.0 0.5 1458808 11804 ?
Sl 00:57 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 41312 0.0 0.4 1327680 9752 ?
Sl 00:57 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 41528 0.0 0.3 292064
7028 pts/0 T 00:57 0:00 /bin/systemctl status httpd.service
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 42391 0.0 0.0 222012
1104 pts/0 S+ 01:01 0:00 grep --color=auto httpd

```

Рис. 7: Определение контекста безопасности

4. Посмотрели текущее состояние переключателей SELinux для Apache. (@fig:008)


```
[root@mkonyaeva httpd]# 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_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_redis 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
httpd_mod_auth_ntlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
```

Рис. 8: Текущее состояние переключателей SELinux для Apache

5. Посмотрели статистику по политике с помощью команды seinfo. (@fig:009)

```
[root@mkonyaeva 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
```

Рис. 9: Статистика по политике

6. Определили тип файлов и поддиректорий, находящихся в директории /var/www.
(@fig:010)

```
[root@mkonyaeva 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
:14 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Aug 12 11
:14 html
```

Рис. 10: Тип файлов и поддиректорий в /var/www

7. Определили тип файлов и поддиректорий, находящихся в директории /var/www/html. (@fig:011)

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

Рис. 11: Тип файлов и поддиректорий в /var/www/html

8. Создали файл test.html и проверили его контекст. (@fig:012)

```
[root@mkonyaeva httpd]# touch /var/www/html/test.html
[root@mkonyaeva httpd]# echo '<html>' >> /var/www/html/test.html
[root@mkonyaeva httpd]# echo '<bode> test </body>' >> /var/www/html/test.html
[root@mkonyaeva httpd]# echo '<body> test </body>' >> /var/www/html/test.html
[root@mkonyaeva httpd]# echo '</html>' >> /var/www/html/test.html
[root@mkonyaeva httpd]# ls -lZ /var/www/html/test.html
ls: cannot access '/var/www/html/test.html': No such file or directory
[root@mkonyaeva httpd]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 62 Oct 10 0
1:12 /var/www/html/test.html
```

Рис. 12: Создание test.html

9. Обратились к файлу через веб-сервер. (@fig:013)

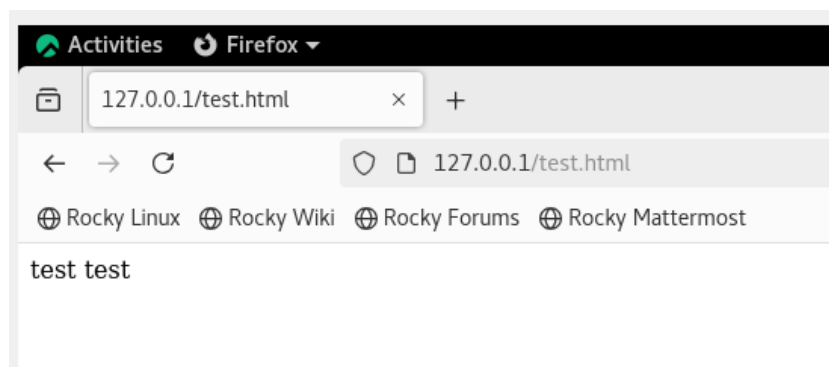


Рис. 13: Обращение к файлу через браузер

10. Изменили контекст файла и проверили что он поменялся. (@fig:014)

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

Рис. 14: Смена контекста test.html

11. Попробовали получить доступ к файлу через браузер. (@fig:015)

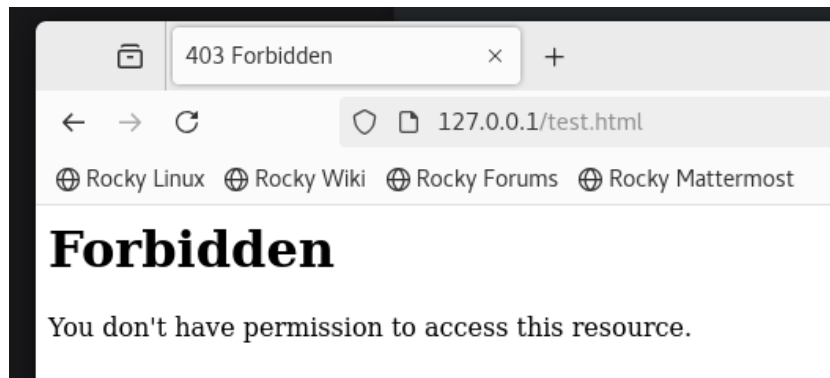


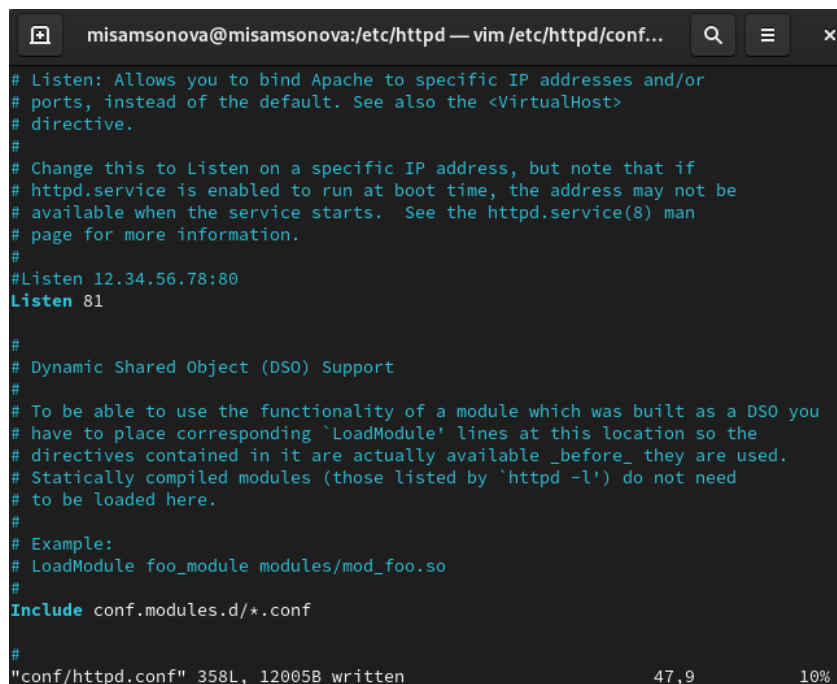
Рис. 15: Обращение к файлу через браузер после смены контекста

12. Просмотрели системный лог-файл. Увидели, что проблема в смененном контексте. (@fig:016)

```
[root@mkonyaeva httpd]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 62 Oct 10 01:12 /var/www/html/test.html
[root@mkonyaeva httpd]# tail /var/log/messages
Oct 10 01:16:42 mkonyaeva systemd[1]: Started SETroubleshoot daemon for processi
ng new SELinux denial logs.
Oct 10 01:16:44 mkonyaeva setroubleshoot[44215]: failed to retrieve rpm info for
/var/www/html/test.html
Oct 10 01:16:44 mkonyaeva dbus-daemon[784]: [system] Activating service name='or
g.fedoraproject.SetroubleshootPrivileged' requested by ':1.436' (uid=980 pid=442
15 comm="/usr/libexec/platform-python -Es /usr/sbin/setroub" label="system_u:sys
tem_r:setroubleshootd_t:s0") (using servicehelper)
Oct 10 01:16:45 mkonyaeva dbus-daemon[784]: [system] Successfully activated serv
ice 'org.fedoraproject.SetroubleshootPrivileged'
Oct 10 01:16:47 mkonyaeva setroubleshoot[44215]: SELinux is preventing /usr/sbin
/httpd from getattr access on the file /var/www/html/test.html. For complete SEL
inux messages run: sealert -l 25665142-2524-49c7-9220-888d866f13c9
Oct 10 01:16:47 mkonyaeva setroubleshoot[44215]: SELinux is preventing /usr/sbin
/httpd from getattr access on the file /var/www/html/test.html.#012#012***** Pl
ugin restorecon (92.2 confidence) suggests *****#012#012If
you want to fix the label. #012/var/www/html/test.html default label should be h
ttpd_sys_content_t.#012Then you can run restorecon. The access attempt may have
been stopped due to insufficient permissions to access a parent directory in whi
ch case try to change the following command accordingly.#012Do#012# /sbin/restor
econ -v /var/www/html/test.html#012#012***** Plugin public_content (7.83 confid
ence) suggests *****#012#012If you want to treat test.html as p
ublic content#012Then you need to change the label on test.html to public_conten
t_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_content t
'/var/www/html/test.html' #012# restorecon -v '/var/www/html/test.html' #012#012**
*** Plugin catchall (1.41 confidence) suggests *****#012
#012If you believe that httpd should be allowed getattr access on the test.html
file by default #012Then you should report this as a bug #012You can generate a
```

Рис. 16: Просмотр системного лог-файла

13. Поменяли прослушивание TCP-порта на 81. (@fig:017)



```
misamsonova@misamsonova:/etc/httpd — vim /etc/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 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
#
"conf/httpd.conf" 358L, 12005B written 47,9 10%
```

Рис. 17: Изменение прослушивания TCP-порта

14. Перезапустили Apache, не получили ошибки. (@fig:018)

```
[root@mkonyaeva httpd]# systemctl restart httpd
[root@mkonyaeva httpd]# tail -n1 /var/log/messages
tail: invalid number of lines: 'l'
[root@mkonyaeva httpd]# tail -n1 /var/log/messages
Oct 10 01:24:45 mkonyaeva httpd[44757]: Server configured, listening on: port
```

Рис. 18: Перезапуск Apache

15. Добавили порт 81 и проверили, что он появился в списке. (@fig:019)

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

Рис. 19: Добавление порта 81

16. Перезапустили Apache, вернули изначальный контекст test.html. (@fig:020)

```
[root@mkonyaeva httpd]# systemctl restart httpd
[root@mkonyaeva httpd]# chcon -t httpd_sys_content_t /var/www/html/test.html
```

Рис. 20: Перезапуск Apache, возвращение изначального контекста test.html

17. Обратились к файлу через веб-сервер. (@fig:021)

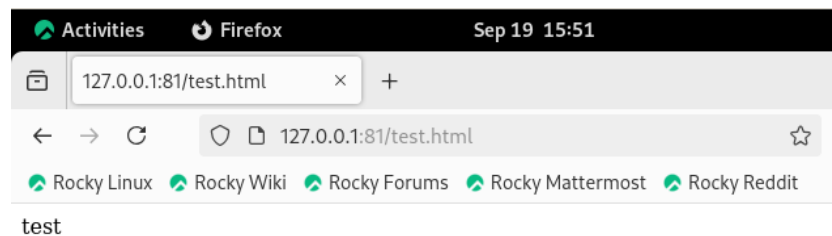
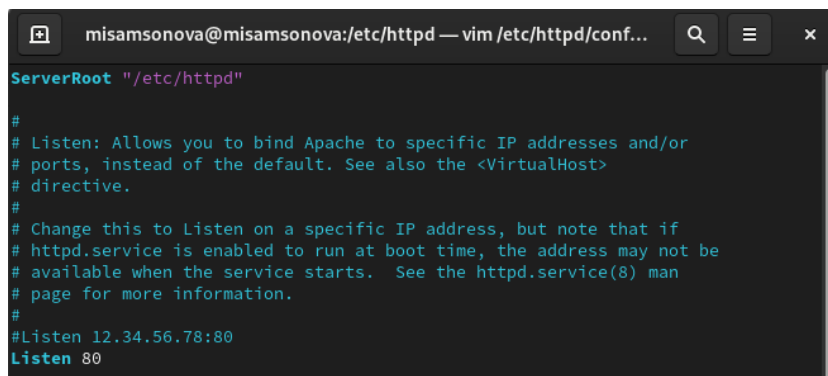


Рис. 21: Обращение к файлу через браузер после возвращения контекста

18. Вернули порт 80. (@fig:022)



```
misamsonova@misamsonova:/etc/httpd — vim /etc/httpd/conf...
ServerRoot "/etc/httpd"

#
# 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. 22: Возвращение порта 80 в httpd.conf

19. Ввели команду для удаления порта 81 из списка. Удалили файл test.html. (@fig:023)



```
[root@mkonyaeva httpd]# semanage port -d -t http_port_t -p tcp 81
[root@mkonyaeva httpd]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@mkonyaeva httpd]#
```

Рис. 23: Работа команды удаления порта 81 и удаление test.html

Вывод

В ходе выполнения лабораторной работы были развиты навыки администрирования ОС Linux и проверена работа SELinux на практике совместно с веб-сервером Apache.

Список литературы. Библиография

[1] Методические материалы курса.

[2] Wikipedia: SELinux (URL: <https://ru.wikipedia.org/wiki/SELinux>)

[3] Wikipedia: Apache HTTP Server (URL: https://ru.wikipedia.org/wiki/Apache_HTTP_Server)3.