

Отчёт по лабораторной работе №6

Информационная безопасность

Мандатное разграничение прав в Linux

Выполнила: Самсонова Мария Ильинична,
НФИбд-02-21, 1032216526

Содержание

Теоретическое введение	4
Цель работы	5
Выполнение лабораторной работы	6
Подготовка лабораторного стенда	6
Основная часть	7
Вывод	16
Список литературы. Библиография	17

Список иллюстраций

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

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]

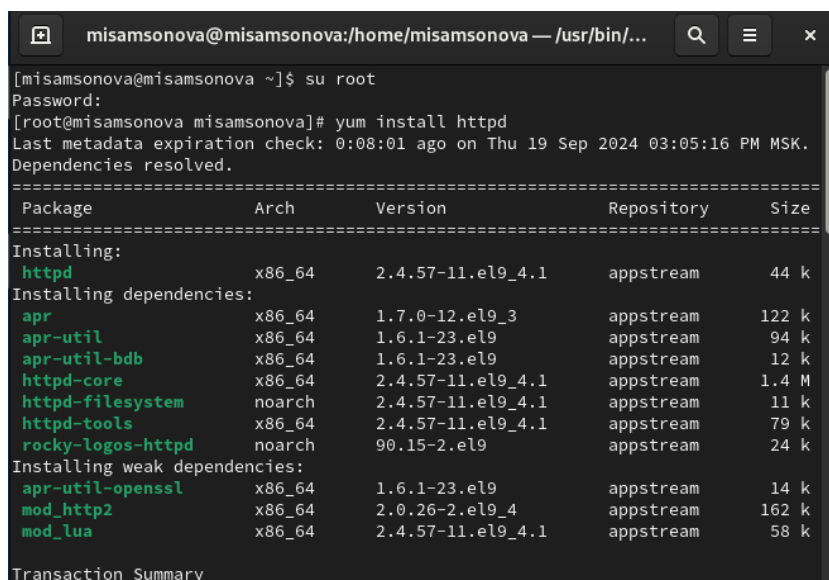
Цель работы

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)

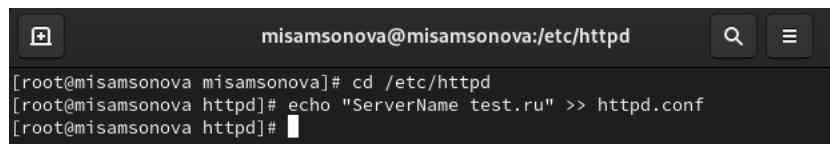


```
[misamsonova@misamsonova ~]$ su root
Password:
[root@misamsonova misamsonova]# yum install httpd
Last metadata expiration check: 0:08:01 ago on Thu 19 Sep 2024 03:05:16 PM MSK.
Dependencies resolved.
=====
Package                Arch      Version      Repository    Size
=====
Installing:
httpd                  x86_64    2.4.57-11.el9_4.1  appstream    44 k
Installing dependencies:
apr                    x86_64    1.7.0-12.el9_3    appstream    122 k
apr-util               x86_64    1.6.1-23.el9      appstream    94 k
apr-util-bdb           x86_64    1.6.1-23.el9      appstream    12 k
httpd-core             x86_64    2.4.57-11.el9_4.1  appstream    1.4 M
httpd-filesystem       noarch    2.4.57-11.el9_4.1  appstream    11 k
httpd-tools            x86_64    2.4.57-11.el9_4.1  appstream    79 k
rocky-logos-httpd      noarch    90.15-2.el9        appstream    24 k
Installing weak dependencies:
apr-util-openssl       x86_64    1.6.1-23.el9      appstream    14 k
mod_http2              x86_64    2.0.26-2.el9_4    appstream    162 k
mod_lua                x86_64    2.4.57-11.el9_4.1  appstream    58 k
Transaction Summary

```

Рис. 1: Установка httpd

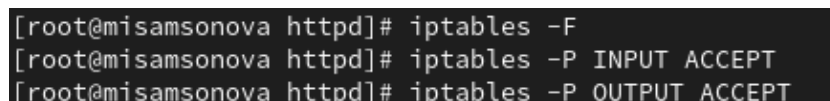
2. В конфигурационном файле /etc/httpd/httpd.conf необходимо задали параметр ServerName. (@fig:002)



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

Рис. 2: Задача параметра ServerName

3. Отключили фильтры. (@fig:003)

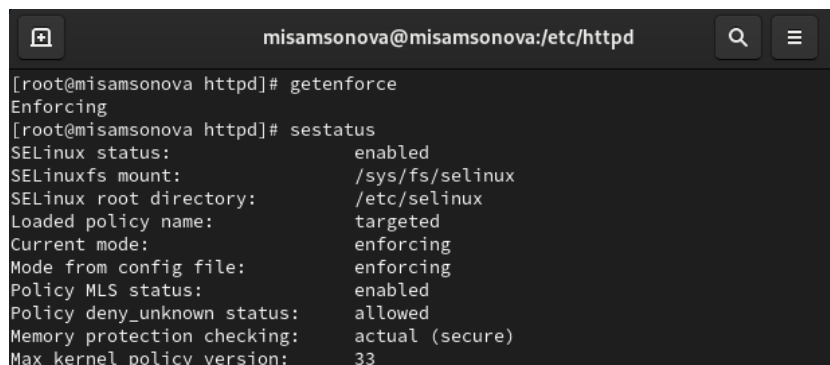


```
[root@misamsonova httpd]# iptables -F
[root@misamsonova httpd]# iptables -P INPUT ACCEPT
[root@misamsonova httpd]# iptables -P OUTPUT ACCEPT
```

Рис. 3: Отключение фильтров

Основная часть

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



```
misamsonova@misamsonova:/etc/httpd
[root@misamsonova httpd]# getenforce
Enforcing
[root@misamsonova 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
```

Рис. 4: Режим работы SELinux

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

```
misamsonova@misamsonova:/etc/httpd
[root@misamsonova 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; preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd.service(8)
```

Рис. 5: Проверка работы сервера

```
[root@misamsonova httpd]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@misamsonova 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; preset: disabled)
   Active: active (running) since Thu 2024-09-19 15:21:46 MSK; 5s ago
     Docs: man:httpd.service(8)
  Main PID: 47762 (httpd)
    Status: "Started, listening on: port 80"
    Tasks: 177 (limit: 10978)
   Memory: 40.3M
      CPU: 772ms
   CGroup: /system.slice/httpd.service
           └─47762 /usr/sbin/httpd -DFOREGROUND
             └─47763 /usr/sbin/httpd -DFOREGROUND
               └─47767 /usr/sbin/httpd -DFOREGROUND
                 └─47768 /usr/sbin/httpd -DFOREGROUND
                   └─47770 /usr/sbin/httpd -DFOREGROUND

Sep 19 15:21:45 misamsonova.localdomain systemd[1]: Starting The Apache HTTP Server:
Sep 19 15:21:46 misamsonova.localdomain systemd[1]: Started The Apache HTTP Server:
Sep 19 15:21:46 misamsonova.localdomain httpd[47762]: Server configured, listening on: port 80
```

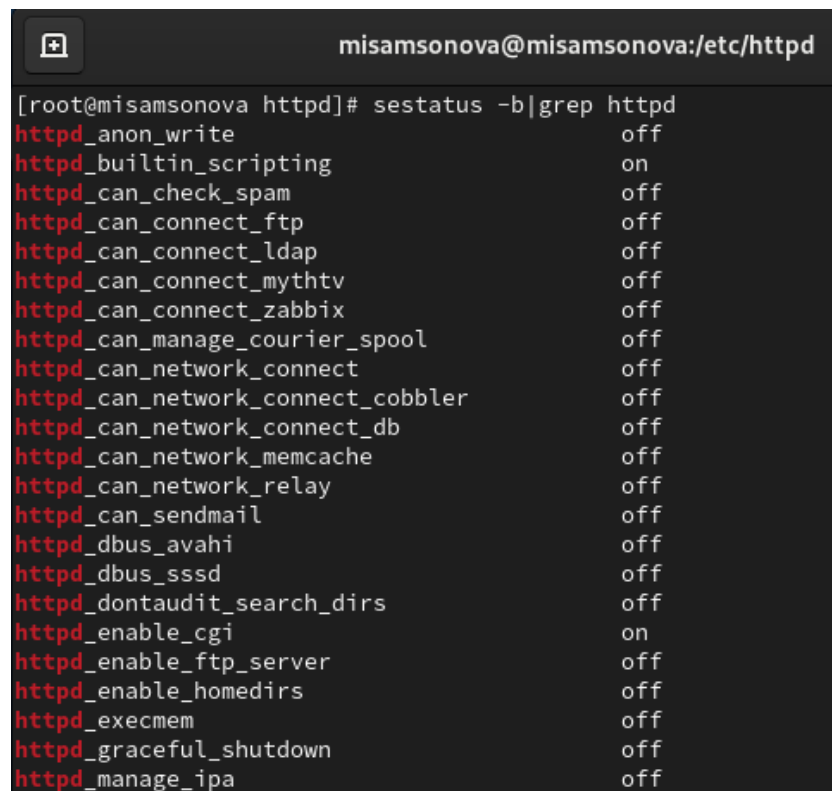
Рис. 6: Запуск сервера

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

```
misamsonova@misamsonova:/etc/httpd
[root@misamsonova httpd]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root      47762  0.4  0.6 20364 11456 ?
Ss   15:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  47763  0.0  0.4 22096  7632 ?
S    15:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  47767  0.0  0.9 1112656 17732 ?
Sl   15:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  47768  0.0  1.0 981520 19572 ?
Sl   15:21   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache  47770  0.0  0.9 981520 17412 ?
Sl   15:21   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 48006 0.0 0.1 221796
2304 pts/1 R+ 15:23   0:00 grep --color=auto httpd
```

Рис. 7: Определение контекста безопасности

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

A terminal window with a dark background and light text. The title bar shows a window icon and the text 'misamsonova@misamsonova:/etc/httpd'. The prompt is '[root@misamsonova httpd]#'. The command 'sestatus -b|grep httpd' has been executed, resulting in a list of SELinux booleans for the httpd process. The booleans are listed in two columns: the name on the left and the status (on or off) on the right. The names are in red text, and the status is in white text.

```
[root@misamsonova 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_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. 8: Текущее состояние переключателей SELinux для Apache

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

```
misamsonova@misamsonova:/etc/httpd
[root@misamsonova httpd]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          33 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                 135
Permissions:             457
Sensitivities:           1
Categories:              1024
Types:                   5145
Attributes:              259
Users:                   8
Roles:                   15
Booleans:                356
Cond. Expr.:             388
Allow:                   65504
Neverallow:              0
Auditallow:              176
Dontaudit:               8682
Type_trans:              271770
Type_change:             94
Type_member:             37
Range_trans:             5931
Role_allow:              40
Role_trans:              417
Constraints:             70
Validatetrans:           0
MLS Constrain:           72
MLS Val. Tran:           0
Permissives:             4
Polcap:                  6
Defaults:                7
Typebounds:              0
Allowxperm:              0
Neverallowxperm:         0
Auditallowxperm:         0
Dontauditxperm:          0
Ibendportcon:            0
Ibpkeycon:               0
Initial SIDs:            27
Fs_use:                  35
Genfscon:                109
Portcon:                 665
Netifcon:                0
Nodecon:                 0
[root@misamsonova httpd]#
```

Рис. 9: Статистика по политике

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

```
misamsonova@misamsonova:/etc/httpd
[root@misamsonova 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 8 19
:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Aug 8 19
:30 html
```

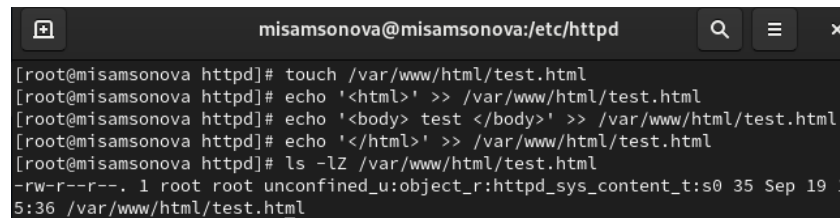
Рис. 10: Тип файлов и поддиректорий в /var/www

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

```
[root@misamsonova 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)

A terminal window titled 'misamsonova@misamsonova:/etc/httpd' showing the following commands and output:

```
[root@misamsonova httpd]# touch /var/www/html/test.html
[root@misamsonova httpd]# echo '<html>' >> /var/www/html/test.html
[root@misamsonova httpd]# echo '<body> test </body>' >> /var/www/html/test.html
[root@misamsonova httpd]# echo '</html>' >> /var/www/html/test.html
[root@misamsonova httpd]# ls -lZ /var/www/html/test.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 35 Sep 19 15:36 /var/www/html/test.html
```

Рис. 12: Создание test.html

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

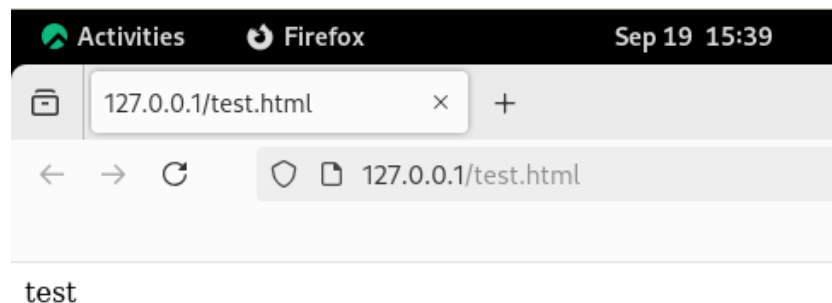
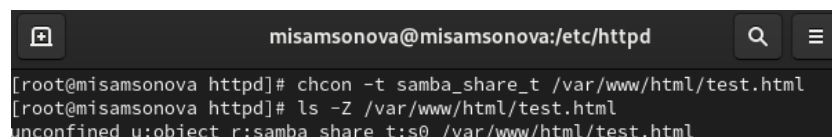


Рис. 13: Обращение к файлу через браузер

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

A terminal window titled 'misamsonova@misamsonova:/etc/httpd' showing the following commands and output:

```
[root@misamsonova httpd]# chcon -t samba_share_t /var/www/html/test.html
[root@misamsonova 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)

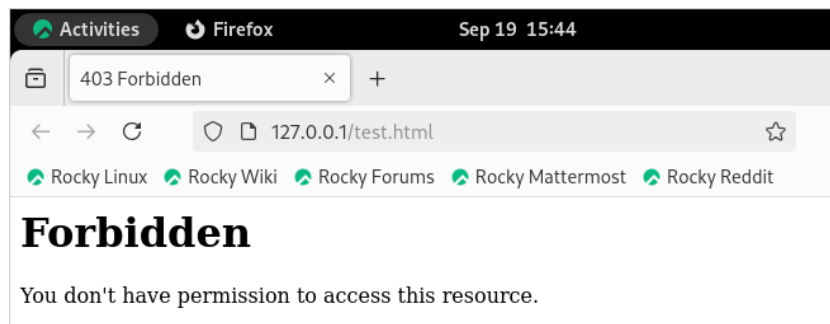


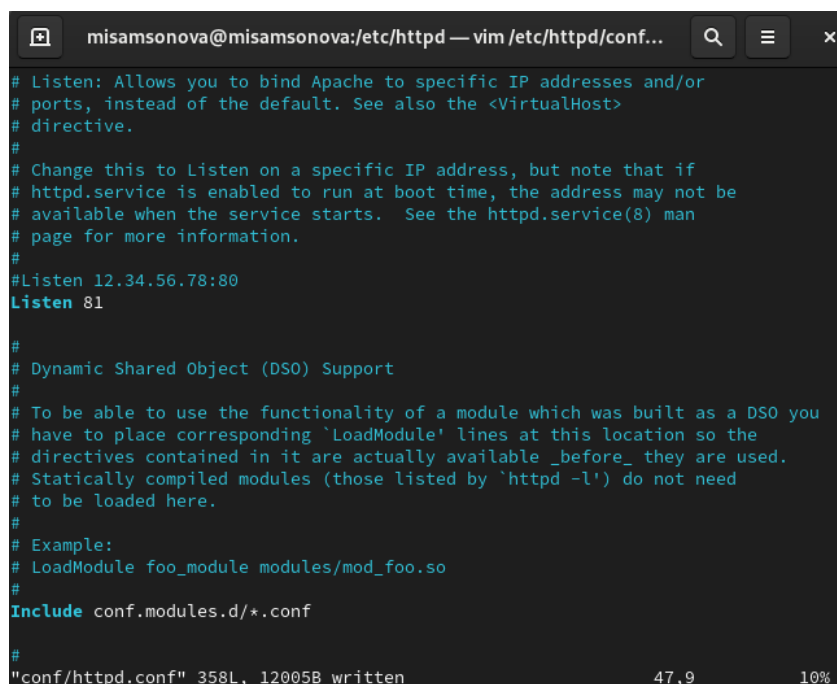
Рис. 15: Обращение к файлу через браузер после смены контекста

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

```
[root@misamsonova httpd]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 35 Sep 19 15:36 /var/www/html/test.html
[root@misamsonova httpd]# tail /var/log/messages
Sep 19 15:44:01 misamsonova systemd[1]: Starting SETroubleshoot daemon for processing new SELinux denial logs...
Sep 19 15:44:09 misamsonova systemd[1]: Started SETroubleshoot daemon for processing new SELinux denial logs.
Sep 19 15:44:13 misamsonova setroubleshoot[48933]: failed to retrieve rpm info for path '/var/www/html/test.html':
Sep 19 15:44:13 misamsonova systemd[1]: Created slice Slice /system/dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged.
Sep 19 15:44:13 misamsonova systemd[1]: Started dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service.
Sep 19 15:44:22 misamsonova systemd[1]: setroubleshootd.service: Deactivated successfully.
Sep 19 15:44:22 misamsonova systemd[1]: setroubleshootd.service: Consumed 6.279s CPU time.
Sep 19 15:44:29 misamsonova systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Deactivated successfully.
Sep 19 15:44:29 misamsonova systemd[1]: dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@0.service: Consumed 9.352s CPU time.
Sep 19 15:44:57 misamsonova gnome-shell[46267]: libinput error: client bug: timer event5 debounce short: scheduled expiry is in the past (-2ms), your system is too slow
```

Рис. 16: Просмотр системного лог-файла

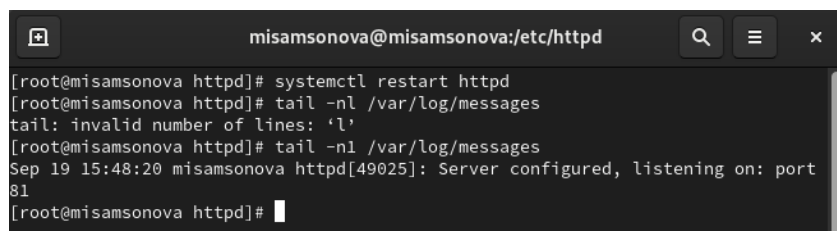
13. Поменяли прослушивание TCP-порта на 81. (@fig:017)



```
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, 120058 written 47,9 10%
```

Рис. 17: Изменение прослушивания TCP-порта

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



```
misamsonova@misamsonova:/etc/httpd
[root@misamsonova httpd]# systemctl restart httpd
[root@misamsonova httpd]# tail -n1 /var/log/messages
tail: invalid number of lines: '1'
[root@misamsonova httpd]# tail -n1 /var/log/messages
Sep 19 15:48:20 misamsonova httpd[49025]: Server configured, listening on: port
81
[root@misamsonova httpd]#
```

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]#
```

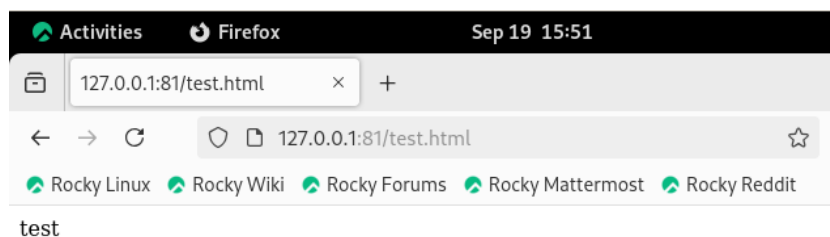
Рис. 19: Добавление порта 81

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

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

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

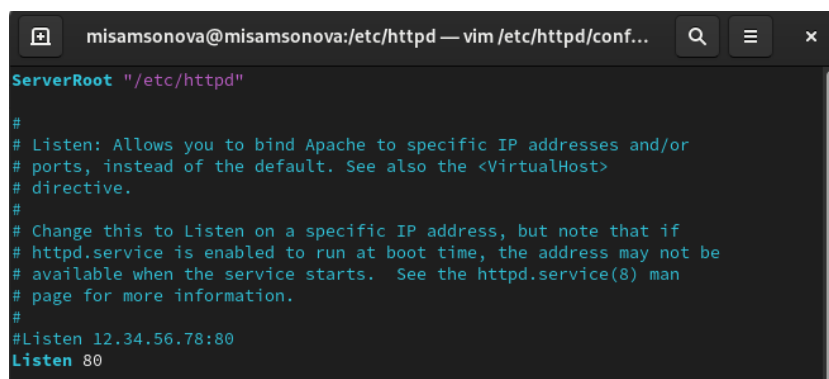
17. Обратились к файлу через веб-сервер. (@fig:021)



The screenshot shows a Firefox browser window with the title 'Sep 19 15:51'. The address bar displays '127.0.0.1:81/test.html'. Below the address bar, there are several bookmarks: 'Rocky Linux', 'Rocky Wiki', 'Rocky Forums', 'Rocky Mattermost', and 'Rocky Reddit'. The main content area of the browser shows the text 'test'.

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

18. Вернули порт 80. (@fig:022)

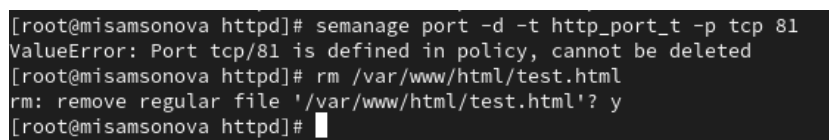


```
misamsonova@misamsonova:/etc/httpd — vim /etc/httpd/conf...
ServerRoot "/etc/httpd"

#
# 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@misamsonova httpd]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@misamsonova httpd]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@misamsonova 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.