

# **Лабораторная работа № 6**

**Дисциплина: Информационная безопасность**

Сулицкий Богдан Романович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
<b>3</b>	<b>Вывод</b>	<b>13</b>
	<b>Список литературы</b>	<b>14</b>

# Список иллюстраций

2.1	Getenforce, sestatus и service status . . . . .	5
2.2	Apache в списке процессов и состояния переключателей . . . . .	6
2.3	Статистика по политике . . . . .	6
2.4	Проверка данных /var/www/ и /var/www/html . . . . .	7
2.5	Содержимое файла test.html . . . . .	7
2.6	Проверка контекста файла . . . . .	7
2.7	Отображение файла в браузере 1 . . . . .	8
2.8	Изменение контекста файла test.html 1 . . . . .	8
2.9	Отображение файла в браузере 2 . . . . .	9
2.10	Просмотр информации о файле test.html и вывод log-файлов . . . . .	9
2.11	Изменения порта 1 . . . . .	10
2.12	Перезапуск веб-сервера 1 . . . . .	10
2.13	Access_log и error_log . . . . .	10
2.14	Привязка порта и проверка списка портов . . . . .	10
2.15	Перезапуск веб-сервера 2 . . . . .	11
2.16	Изменение контекста файла test.html 2 . . . . .	11
2.17	Отображение файла в браузере 3 . . . . .	11
2.18	Изменения порта 2 . . . . .	12
2.19	Удаление привязки порта и удаление файла test.html . . . . .	12

# 1 Цель работы

Целью данной лабораторной работы является развитие навыков администрирования ОС Linux и получение первого практического знакомства с технологией SELinux

## 2 Выполнение лабораторной работы

1. Я вошёл в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted. Далее я убедился, что веб-сервер работает(2.1).

```
[root@localhost user]# getenforce
Enforcing
[root@localhost 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
Max kernel policy version:    31
[root@localhost 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 preset: disabled)
   Active: active (running) since Sat 2023-10-14 18:43:12 MSK; 14min ago
```

Рис. 2.1: Getenforce, sestatus и service status

2. Я нашёл веб-сервер Apache в списке процессов и посмотрел текущее состояние переключателей SELinux для Apache(2.2).

```
[root@localhost user]# ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 10339 0.0 0.2 224088 5060 ? Ss 18:43 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 10340 0.0 0.1 226172 3100 ? S 18:43 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 10341 0.0 0.1 226172 3100 ? S 18:43 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 10342 0.0 0.1 226172 3100 ? S 18:43 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 10343 0.0 0.1 226172 3100 ? S 18:43 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 10344 0.0 0.1 226172 3100 ? S 18:43 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 10785 0.0 0.0 112808 968 pts/1 R+ 18:57 0:00 grep --color=auto httpd
[root@localhost 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_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. 2.2: Араше в списке процессов и состояния переключателей

3. Я посмотрел статистику по политике с помощью команды seinfo: 4793 типа, 8 пользователей и 14 ролей(2.3).

```
[root@localhost user]# seinfo

Statistics for policy file: /sys/fs/selinux/policy
Policy Version & Type: v.31 (binary, mls)

Classes: 130 Permissions: 272
Sensitivities: 1 Categories: 1024
Types: 4793 Attributes: 253
Users: 8 Roles: 14
Booleans: 316 Cond. Expr.: 362
Allow: 107834 Neverallow: 0
Auditallow: 158 Dontaudit: 10022
Type_trans: 18153 Type_change: 74
Type_member: 35 Role_allow: 37
Role_trans: 414 Range_trans: 5899
Constraints: 143 Validatetrans: 0
Initial SIDs: 27 Fs_use: 32
Genfscon: 103 Portcon: 614
Netifcon: 0 Nodecon: 0
Permissives: 0 Polcap: 5
```

Рис. 2.3: Статистика по политике

4. Я определил тип файлов и поддиректорий, находящихся в директории /var/www. Далее я определил тип файлов в директории /var/www/html, и круг пользователей, которым разрешено создание файлов(2.4).

```
[root@localhost user]# ls -lZ /var/www
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
[root@localhost user]# ls -lZ /var/www/html
[root@localhost user]#
```

Рис. 2.4: Проверка данных /var/www/ и /var/www/html

5. Я создал от имени суперпользователя html-файл(2.5).

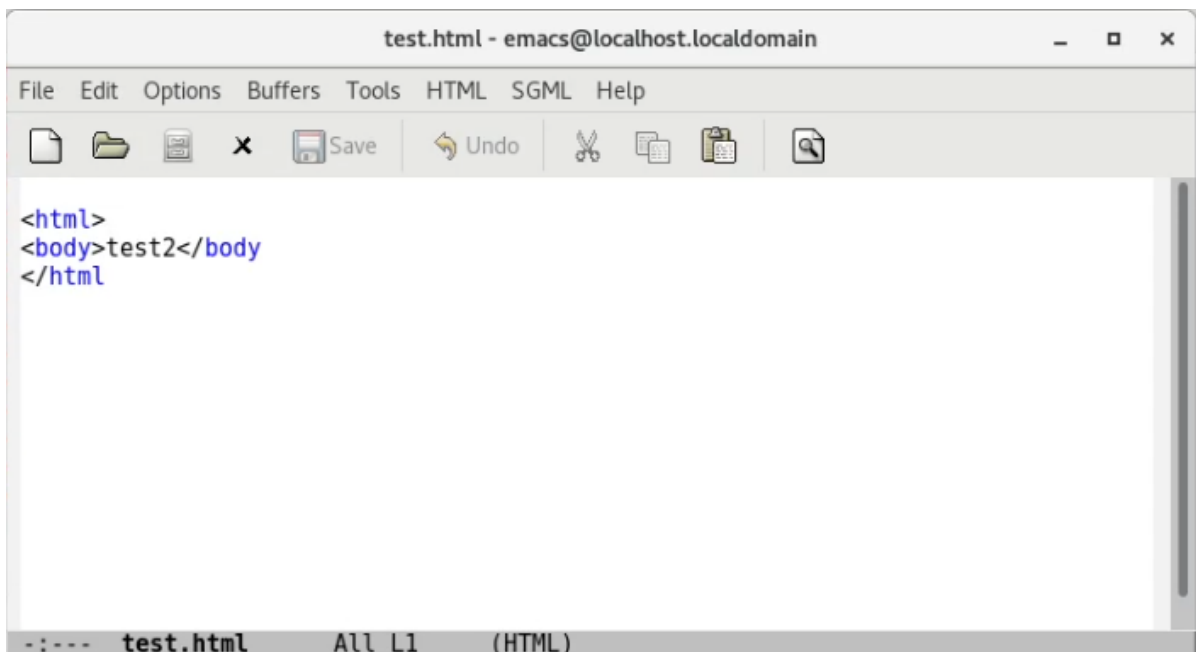


Рис. 2.5: Содержимое файла test.html

6. Я проверил контекст созданного мною файла(2.6).

```
[root@localhost user]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Рис. 2.6: Проверка контекста файла

7. Я обратился к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1/test.html>.(2.7)

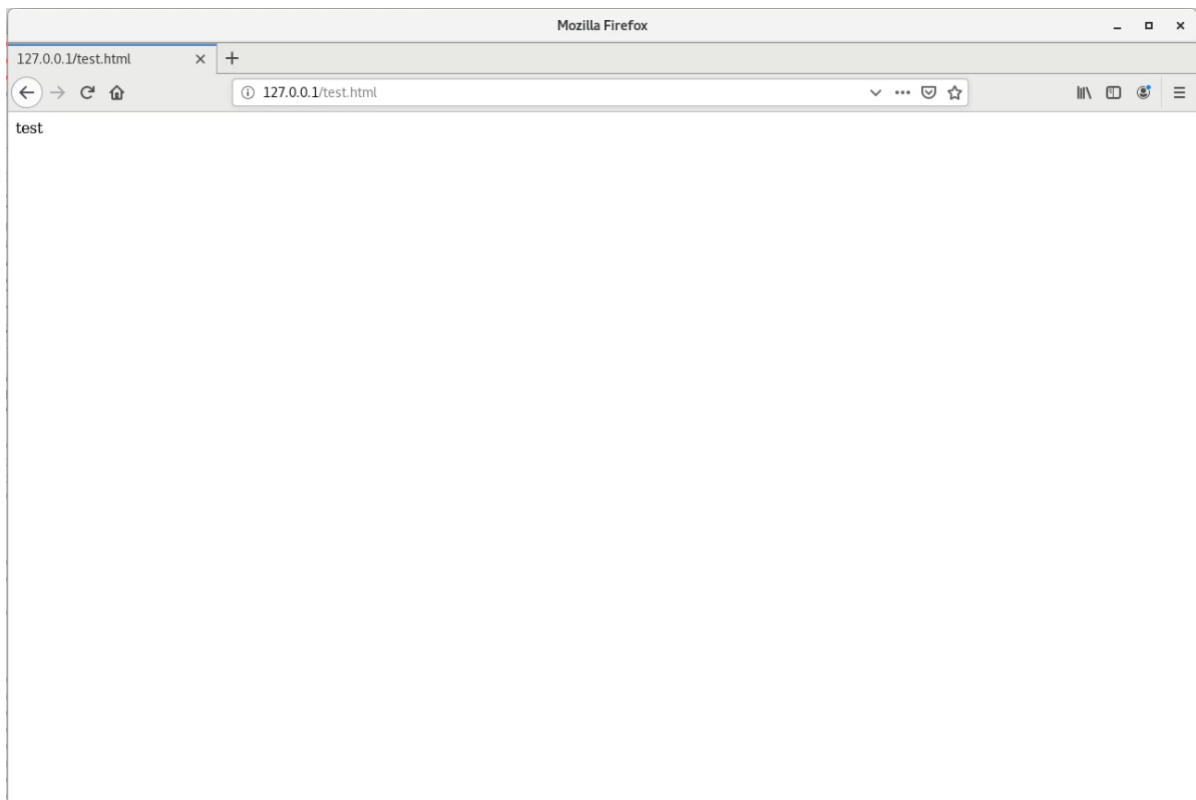


Рис. 2.7: Отображение файла в браузере 1

Файл был успешно отображён.

8. Я попробовал изучить справку `man httpd_selinux`, однако получил ошибку.  
Далее я изменил контекст файла `test.html` на `samba_share_t(2.8)`.

```
No manual entry for httpd_selinux
[root@localhost user]# chcon -t sambe_share_t /var/www/html/test.html
chcon: failed to change context of '/var/www/html/test.html' to 'unconfined_u:object_r:sambe_share_t:s0': Invalid argument
[root@localhost user]# chcon -t samba_share_t /var/www/html/test.html
[root@localhost user]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
```

Рис. 2.8: Изменение контекста файла `test.html` 1

9. Я обратился к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`.  
Получил ошибку `Forbidden(2.9)`.



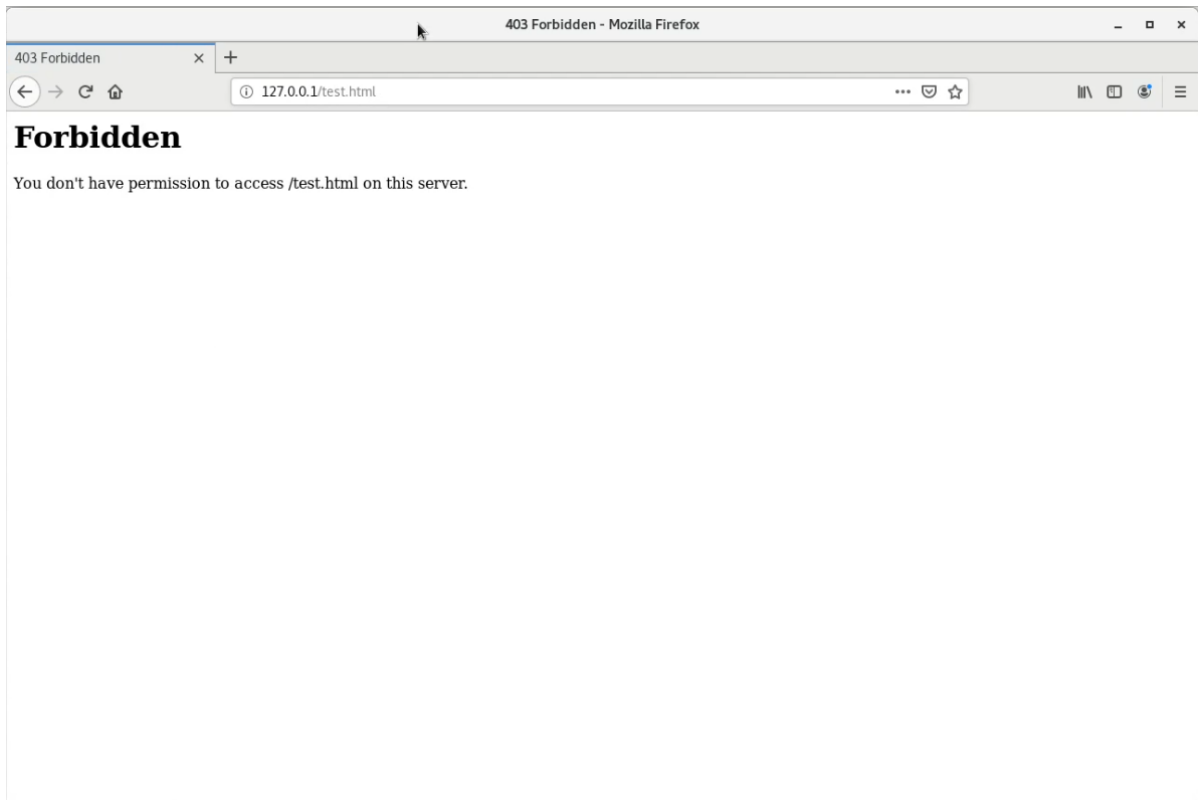


Рис. 2.9: Отображение файла в браузере 2

## 10. Я изучил права доступа на файл test.html, просмотрел log-файлы и файл аудита(2.10).

```
[root@localhost user]# ls -l /var/www/html/test.html
-rw-r--r-- 1 root root 33 Oct 14 18:06 /var/www/html/test.html
[root@localhost user]# tail /var/log/messages
Oct 14 19:13:37 localhost dbus[741]: [system] Activating service name='org.fedoraproject.Setroubleshoo' (using servicehelper)
Oct 14 19:13:37 localhost dbus[741]: [system] Successfully activated service 'org.fedoraproject.Setroubleshoo'
Oct 14 19:13:37 localhost setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 14 19:13:37 localhost setroubleshoot: SELinux is preventing httpd from getatrr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l cfa42836-f523-417f-9f86-f13433e34d45
Oct 14 19:13:37 localhost python: SELinux is preventing httpd from getatrr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****#012#01
2If you want to fix the label. #012/var/www/html/test.html default label should be httpd_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 which case try to change the following command accordingly.#0120#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public content (7.83 confidence) suggests *
*****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.html to public content_t or public content_rw_t.#0120#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 getatrr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#0120#012allow this access for now by executing:#
012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
Oct 14 19:13:49 localhost dbus[741]: [system] Activating service name='org.fedoraproject.Setroubleshoo' (using servicehelper)
Oct 14 19:13:50 localhost setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 14 19:13:50 localhost setroubleshoot: SELinux is preventing httpd from getatrr access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l cfa42836-f523-417f-9f86-f13433e34d45
Oct 14 19:13:50 localhost python: SELinux is preventing httpd from getatrr access on the file /var/www/html/test.html.#012#012***** Plugin restorecon (92.2 confidence) suggests *****#012#01
2If you want to fix the label. #012/var/www/html/test.html default label should be httpd_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 which case try to change the following command accordingly.#0120#012# /sbin/restorecon -v /var/www/html/test.html#012#012***** Plugin public content (7.83 confidence) suggests *
*****#012#012If you want to treat test.html as public content#012Then you need to change the label on test.html to public content_t or public content_rw_t.#0120#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 getatrr access on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local policy module to allow this access.#0120#012allow this access for now by executing:#
012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -i my-httpd.pp#012
[root@localhost user]# tail /var/log/audit/audit.log
type=AVC msg=audit(1697299978.659:3070): avc: denied { mac_admin } for pid=12116 comm="chcon" capability=33 scontext=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 tcontext=unconfined_u:unconfined_r:u
nconfined_t:s0-s0:c0.c1023 tclass=capability2 permissive=0
type=SELINUX_ERR msg=audit(1697299978.659:3070): op=setattr invalid context="unconfined_u:object_r:samba_share_t:s0"
type=SYSCALL msg=audit(1697299978.659:3070): arch=c000003e syscall=188 success=no exit=-22 a0=10cd00 a1=7f5682dda6a a2=10ce5d0 a3=27 items=0 ppid=10676 pid=12116 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0
type=PROCTITLE msg=audit(1697299978.659:3070): proctitle=2F7573722F7362696E2F6874747064002044464F524547524F554E44
type=AVC msg=audit(1697300014.464:3071): avc: denied { getattr } for pid=11958 comm="httpd" path="/var/www/html/test.html" dev="dm-0" ino=51963483 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:0
bject_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1697300014.464:3071): arch=c000003e syscall=4 success=no exit=-13 a0=55821db1e360 a1=7fff948db780 a2=7fff948db780 a3=7fb57a0b7772 items=0 ppid=11957 pid=11958 auid=4294967295 uid=48 gid=48
euid=48 fsuid=48 egid=48 fsuid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)
type=PROCTITLE msg=audit(1697300014.464:3071): proctitle=2F7573722F7362696E2F6874747064002044464F524547524F554E44
type=AVC msg=audit(1697300014.464:3072): avc: denied { getattr } for pid=11958 comm="httpd" path="/var/www/html/test.html" dev="dm-0" ino=51963483 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:0
bject_r:samba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1697300014.464:3072): arch=c000003e syscall=6 success=no exit=-13 a0=55821db1e440 a1=7fff948db780 a2=7fff948db780 a3=0 items=0 ppid=11957 pid=11958 auid=4294967295 uid=48 gid=48 suid=48 fsuid=48 egid=48 fsuid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)
type=PROCTITLE msg=audit(1697300014.464:3072): proctitle=2F7573722F7362696E2F6874747064002044464F524547524F554E44
```

Рис. 2.10: Просмотр информации о файле test.html и вывод log-файлов

Audit.log и log-файлы содержат в себе данные об отказе в доступе.

11. Я попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81(2.11).

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

Рис. 2.11: Изменения порта 1

И попробовал перезапустить веб-сервер(2.12).

```
[root@localhost user]# systemctl restart httpd
[root@localhost user]# tail -n1 /var/log/messages
Oct 14 19:22:14 localhost systemd: Started The Apache HTTP Server.
```

Рис. 2.12: Перезапуск веб-сервера 1

Сервер перезапустился. Никаких сбоев не было, так 81 порт по умолчанию используется в пуле.

12. Я проанализировал лог-файлы(2.13).

```
[root@localhost user]# tail /var/log/httpd/access_log
127.0.0.1 - - [14/Oct/2023:15:34:43 +0300] "GET /test.html HTTP/1.1" 403 211 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [14/Oct/2023:15:34:43 +0300] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [14/Oct/2023:17:30:41 +0300] "GET /test.html HTTP/1.1" 200 31 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [14/Oct/2023:17:39:25 +0300] "GET /test2.html HTTP/1.1" 200 32 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [14/Oct/2023:17:43:28 +0300] "GET /test.html HTTP/1.1" 200 31 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [14/Oct/2023:17:43:28 +0300] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [14/Oct/2023:17:43:43 +0300] "GET /test.html HTTP/1.1" 403 211 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [14/Oct/2023:18:16:19 +0300] "GET /test.html HTTP/1.1" 200 31 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [14/Oct/2023:19:09:34 +0300] "GET /test.html HTTP/1.1" 200 33 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
127.0.0.1 - - [14/Oct/2023:19:13:34 +0300] "GET /test.html HTTP/1.1" 403 211 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
[root@localhost user]# tail /var/log/httpd/error_log
[Sat Oct 14 19:09:29.964983 2023] [mpm_prefork:notice] [pid 11957] AH00163: Apache/2.4.6 (CentOS) configured -- resuming normal operations
[Sat Oct 14 19:09:29.964997 2023] [core:notice] [pid 11957] AH00894: Command Line: '/usr/sbin/httpd -D FOREGROUND'
[Sat Oct 14 19:13:34.405230 2023] [core:error] [pid 11958] (13)Permission denied: [client 127.0.0.1:48718] AH00035: access to /test.html denied (filesystem path '/var/www/html/test.html') because search permissions are missing on a component of the path
[Sat Oct 14 19:18:12.587504 2023] [mpm_prefork:notice] [pid 11957] AH00170: caught SIGWINCH, shutting down gracefully
[Sat Oct 14 19:18:13.657649 2023] [core:notice] [pid 12529] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0
[Sat Oct 14 19:18:13.658159 2023] [suexec:notice] [pid 12529] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain. Set the 'ServerName' directive globally to suppress this message
[Sat Oct 14 19:18:13.667607 2023] [lbmethod:heartbeat:notice] [pid 12529] AH02282: No slotmem from mod_heartbeat
[Sat Oct 14 19:18:13.669126 2023] [mpm_prefork:notice] [pid 12529] AH00163: Apache/2.4.6 (CentOS) configured -- resuming normal operations
[Sat Oct 14 19:18:13.669146 2023] [core:notice] [pid 12529] AH00894: Command Line: '/usr/sbin/httpd -D FOREGROUND'
```

Рис. 2.13: Access\_log и error\_log

Никаких новых записей не появилось.

13. Я выполнил команду привязки порта и получил ошибку, так как порт уже определен. Далее я проверил список портов(2.14).

```
[root@localhost user]# semanage port -a -t http_port_t -p tcp 81
ValueError: Port tcp/81 already defined
[root@localhost user]# 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
```

Рис. 2.14: Привязка порта и проверка списка портов

14. Я попробовал перезапустить веб-сервер. Он успешно перезапустился, как и в предыдущий раз(2.15).

```
[root@localhost user]# systemctl restart httpd
[root@localhost user]# tail -n1 /var/log/messages
Oct 14 19:22:14 localhost systemd: Started The Apache HTTP Server.
```

Рис. 2.15: Перезапуск веб-сервера 2

15. Я вернул контекст httpd\_sys\_content\_t к файлу test.html(2.16).

```
[root@localhost user]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@localhost user]# ls -lZ /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Рис. 2.16: Изменение контекста файла test.html 2

После этого я попробовал получить доступ к файлу через веб-сервер, введя в браузере адрес <http://127.0.0.1:81/test.html> (2.17).

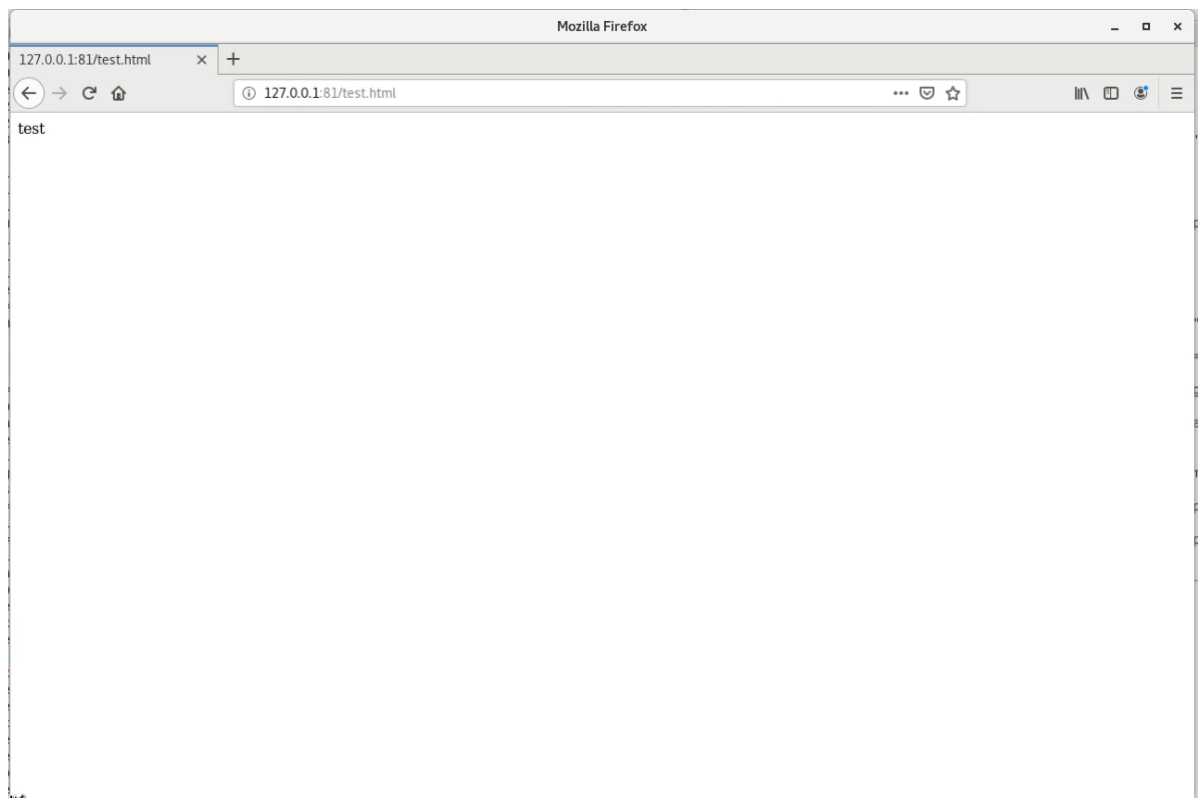


Рис. 2.17: Отображение файла в браузере 3

Файл был успешно отображён.

16. Я исправил обратно конфигурационный файл `apache`, вернув `Listen 80`(2.18).

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

Рис. 2.18: Изменения порта 2

17. Я попробовал удалить привязку `http_port_t` к 81 порту, но поскольку данный порт определен политикой, я не смог исполнить эту команду. Далее я удалил файл `test.html` с помощью команды `rm`(2.19).

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

Рис. 2.19: Удаление привязки порта и удаление файла `test.html`

## 3 Вывод

В ходе проделанной лабораторной работы я развил свои навыки администрирования ОС Linux и получил первое практическое знакомство с технологией SELinux

## Список литературы

[1] [https://esystem.rudn.ru/pluginfile.php/2090282/mod\\_resource/content/2/006-lab\\_selinux.pdf](https://esystem.rudn.ru/pluginfile.php/2090282/mod_resource/content/2/006-lab_selinux.pdf)