

# **Отчёт по лабораторной работе №6**

**Знакомство с SELinux**

Стаменкович Огнен

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
2.1	Подготовка . . . . .	5
2.2	Изучение механики SetUID . . . . .	5
<b>3</b>	<b>Выводы</b>	<b>13</b>
	<b>Список литературы</b>	<b>14</b>

# List of Figures

2.1	запуск http . . . . .	6
2.2	контекст безопасности http . . . . .	6
2.3	переключатели SELinux для http . . . . .	7
2.4	создание html-файла и доступ по http . . . . .	8
2.5	ошибка доступа после изменения контекста . . . . .	9
2.6	лог ошибок . . . . .	10
2.7	переключение порта . . . . .	11
2.8	доступ по http на 81 порт . . . . .	12

# 1 Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache

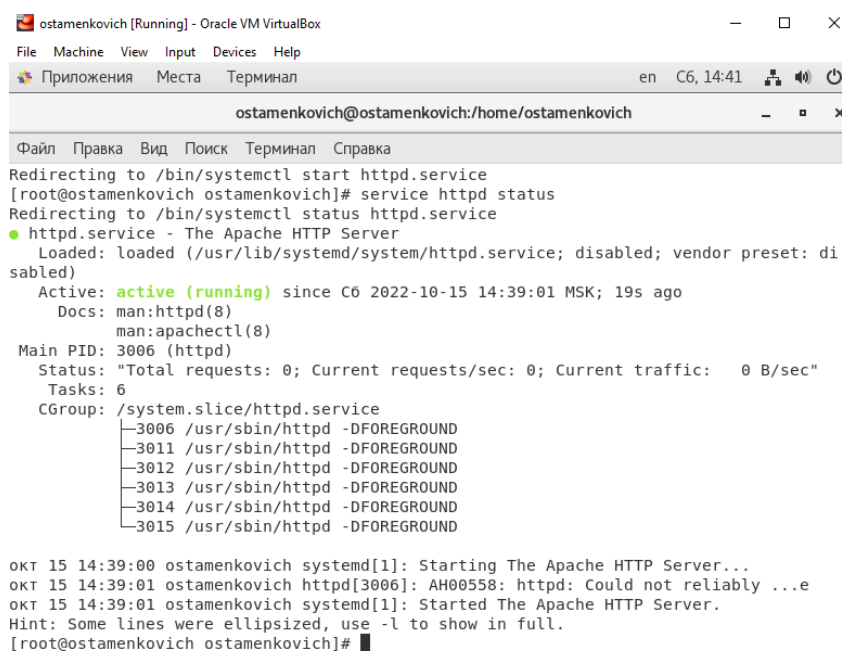
## 2 Выполнение лабораторной работы

### 2.1 Подготовка

1. Установили httpd
2. Задали имя сервера
3. Открыли порты для работы с протоколом http

### 2.2 Изучение механики SetUID

1. Войдите в систему с полученными учётными данными и убедитесь, что SELinux работает в режиме enforcing политики targeted с помощью команд `getenforce` и `sestatus`.
2. Обратитесь с помощью браузера к веб-серверу, запущенному на вашем компьютере, и убедитесь, что последний работает: `service httpd status` или `/etc/rc.d/init.d/httpd status` Если не работает, запустите его так же, но с параметром `start`.

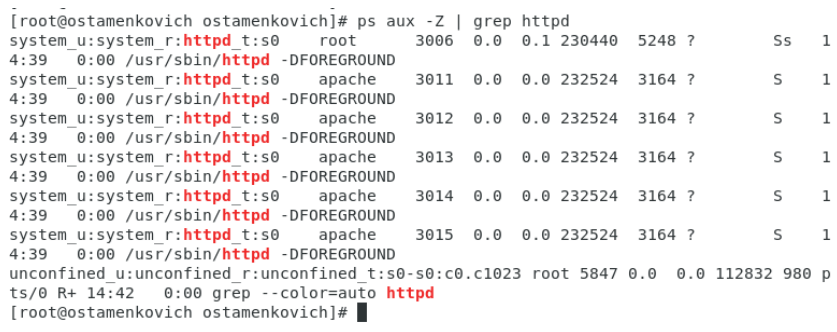


```
ostamenkovich [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Приложения Места Терминал en C6, 14:41
ostamenkovich@ostamenkovich:/home/ostamenkovich
Файл Правка Вид Поиск Терминал Справка
Redirecting to /bin/systemctl start httpd.service
[root@ostamenkovich ostamenkovich]# service 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 C6 2022-10-15 14:39:01 MSK; 19s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Main PID: 3006 (httpd)
    Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
     Tasks: 6
    CGroup: /system.slice/httpd.service
            └─3006 /usr/sbin/httpd -DFOREGROUND
              └─3011 /usr/sbin/httpd -DFOREGROUND
                └─3012 /usr/sbin/httpd -DFOREGROUND
                  └─3013 /usr/sbin/httpd -DFOREGROUND
                    └─3014 /usr/sbin/httpd -DFOREGROUND
                      └─3015 /usr/sbin/httpd -DFOREGROUND

окт 15 14:39:00 ostamenkovich systemd[1]: Starting The Apache HTTP Server...
окт 15 14:39:01 ostamenkovich httpd[3006]: AH00558: httpd: Could not reliably ...e
окт 15 14:39:01 ostamenkovich systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@ostamenkovich ostamenkovich]#
```

Figure 2.1: запуск http

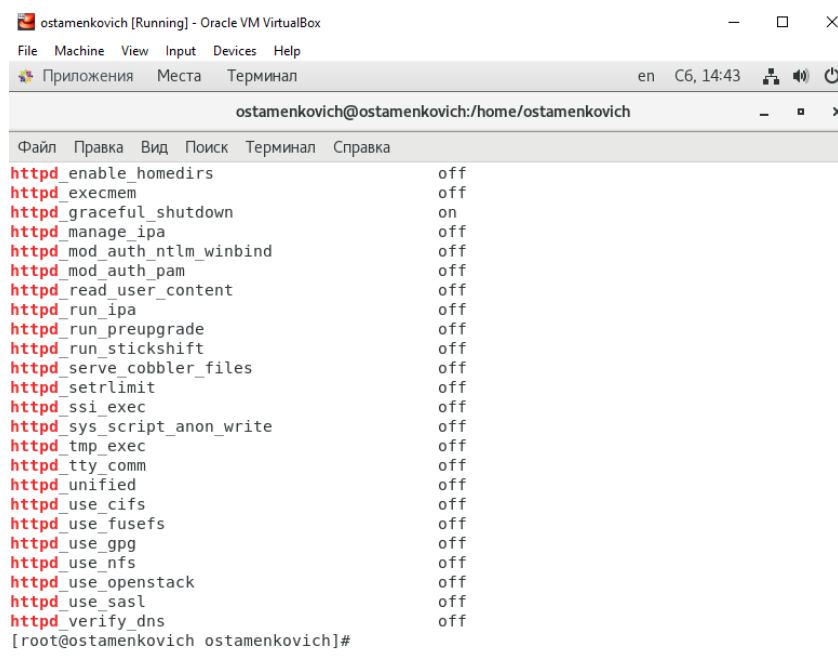
3. Найдите веб-сервер Apache в списке процессов, определите его контекст безопасности и занесите эту информацию в отчёт. Например, можно использовать команду `ps auxZ | grep httpd` или `ps -eZ | grep httpd`



```
[root@ostamenkovich ostamenkovich]# ps aux -Z | grep httpd
system_u:system_r:httpd_t:s0 root 3006 0.0 0.1 230440 5248 ? Ss 1
4:39 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3011 0.0 0.0 232524 3164 ? S 1
4:39 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3012 0.0 0.0 232524 3164 ? S 1
4:39 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3013 0.0 0.0 232524 3164 ? S 1
4:39 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3014 0.0 0.0 232524 3164 ? S 1
4:39 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3015 0.0 0.0 232524 3164 ? S 1
4:39 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 5847 0.0 0.0 112832 980 p
ts/0 R+ 14:42 0:00 grep --color=auto httpd
[root@ostamenkovich ostamenkovich]#
```

Figure 2.2: контекст безопасности http

4. Посмотрите текущее состояние переключателей SELinux для Apache с помощью команды `sestatus -bigrep httpd` Обратите внимание, что многие из них находятся в положении «off».



The screenshot shows a terminal window titled "ostamenkovich [Running] - Oracle VM VirtualBox". The terminal output displays the SELinux status for the httpd process. The status is as follows:

SELinux Process	Status
httpd_enable_homedirs	off
httpd_execmem	off
httpd_graceful_shutdown	on
httpd_manage_ipa	off
httpd_mod_auth_ntlm_winbind	off
httpd_mod_auth_pam	off
httpd_read_user_content	off
httpd_run_ipa	off
httpd_run_preupgrade	off
httpd_run_stickshift	off
httpd_serve_cobbler_files	off
httpd_setrlimit	off
httpd_ssi_exec	off
httpd_sys_script_anon_write	off
httpd_tmp_exec	off
httpd_tty_comm	off
httpd_unified	off
httpd_use_cifs	off
httpd_use_fusefs	off
httpd_use_gpg	off
httpd_use_nfs	off
httpd_use_openstack	off
httpd_use_sasl	off
httpd_verify_dns	off

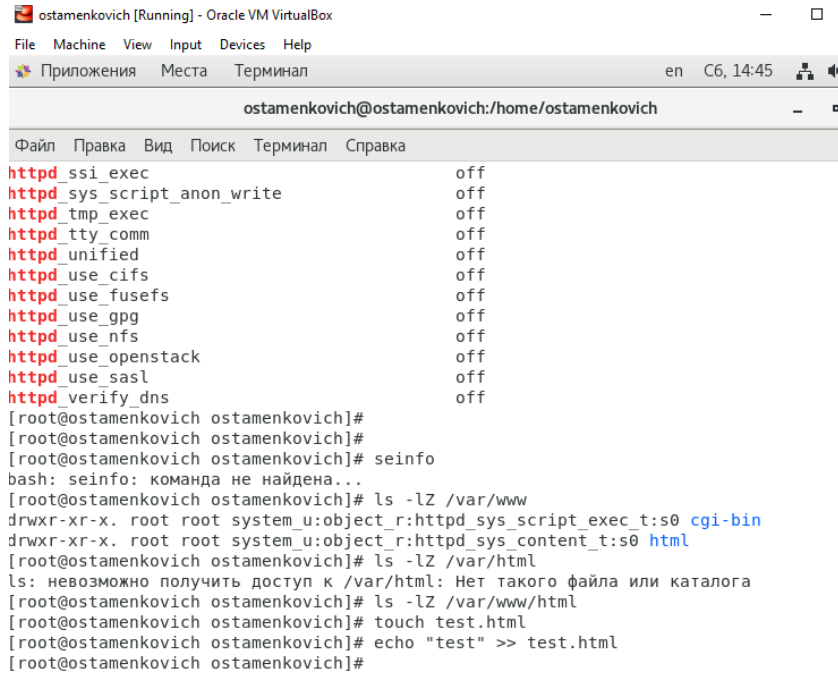
The prompt at the bottom of the terminal is `[root@ostamenkovich ostamenkovich]#`.

Figure 2.3: переключатели SELinux для http

5. Посмотрите статистику по политике с помощью команды `seinfo`, также определите множество пользователей, ролей, типов.
6. Определите тип файлов и поддиректорий, находящихся в директории `/var/www`, с помощью команды `ls -lZ /var/www`. В поддиректориях могут располагаться системные скрипты и контент для http.
7. Определите тип файлов, находящихся в директории `/var/www/html`: `ls -lZ /var/www/html`. В директории изначально нет файлов.
8. Определите круг пользователей, которым разрешено создание файлов в директории `/var/www/html`. Создавать файлы может только root.
9. Создайте от имени суперпользователя (так как в дистрибутиве после установки только ему разрешена запись в директорию) html-файл `/var/www/html/test.html` следующего содержания: Test
10. Проверьте контекст созданного вами файла. Занесите в отчёт контекст, присваиваемый по умолчанию вновь созданным файлам в директории

/var/www/html.

11. Обратитесь к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедитесь, что файл был успешно отображён.



```
ostamenkovich [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Приложения Места Терминал en C6, 14:45
ostamenkovich@ostamenkovich:/home/ostamenkovich
Файл Правка Вид Поиск Терминал Справка
httpd_ssi_exec off
httpd_sys_script_anon_write off
httpd_tmp_exec off
httpd_tty_comm off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_openstack off
httpd_use_sasl off
httpd_verify_dns off
[root@ostamenkovich ostamenkovich]#
[root@ostamenkovich ostamenkovich]#
[root@ostamenkovich ostamenkovich]# seinfo
bash: seinfo: команда не найдена...
[root@ostamenkovich ostamenkovich]# 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@ostamenkovich ostamenkovich]# ls -lZ /var/html
ls: невозможно получить доступ к /var/html: Нет такого файла или каталога
[root@ostamenkovich ostamenkovich]# ls -lZ /var/www/html
[root@ostamenkovich ostamenkovich]# touch test.html
[root@ostamenkovich ostamenkovich]# echo "test" >> test.html
[root@ostamenkovich ostamenkovich]#
```

Figure 2.4: создание html-файла и доступ по http

12. Изучите справку `man httpd_selinux` и выясните, какие контексты файлов определены для `httpd`. Сопоставьте их с типом файла `test.html`. Проверить контекст файла можно командой `ls -Z`. `ls -Z /var/www/html/test.html`. Основным контекстом является `httpd_sys_content_t`, его мы и увидели в выводе команды.
13. Измените контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на любой другой, к которому процесс `httpd` не должен иметь доступа, например, на `samba_share_t`: `chcon -t samba_share_t /var/www/html/test.html` `ls -Z /var/www/html/test.html` После этого проверьте, что контекст поменялся.
14. Попробуйте ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Вы должны получить сообщение об



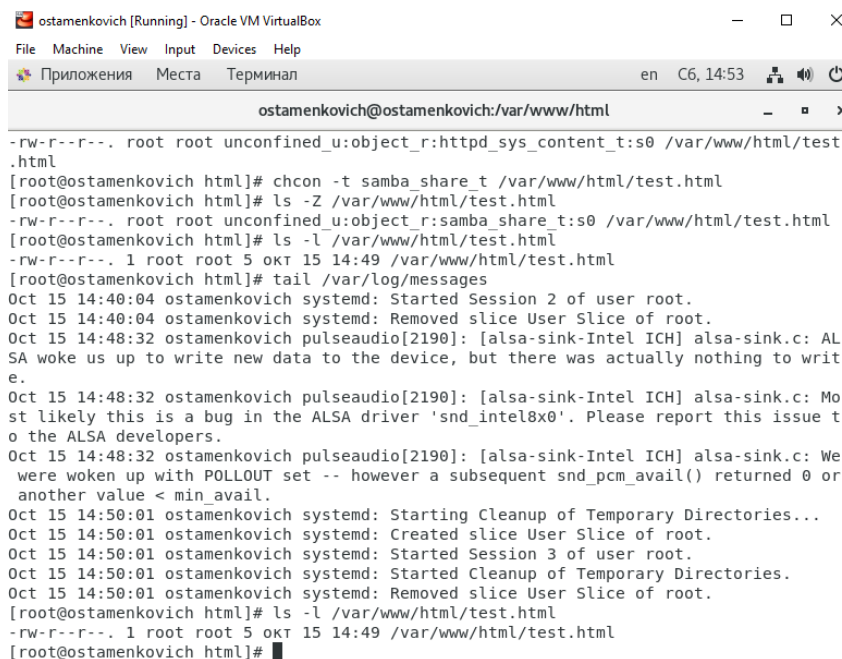
ошибке: Forbidden You don't have permission to access /test.html on this server. При изменении контекста файл стал считаться чужим для http и программа не может его прочитать.

```
[root@ostamenkovich ostamenkovich]# ls -lZ /var/www/html
[root@ostamenkovich ostamenkovich]# cd /var/www/html
[root@ostamenkovich html]# echo "test" >> test.html
[root@ostamenkovich html]#
[root@ostamenkovich html]#
[root@ostamenkovich html]#
[root@ostamenkovich html]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@ostamenkovich html]# chcon -t samba_share_t /var/www/html/test.html
[root@ostamenkovich html]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@ostamenkovich html]#
```

---

Figure 2.5: ошибка доступа после изменения контекста

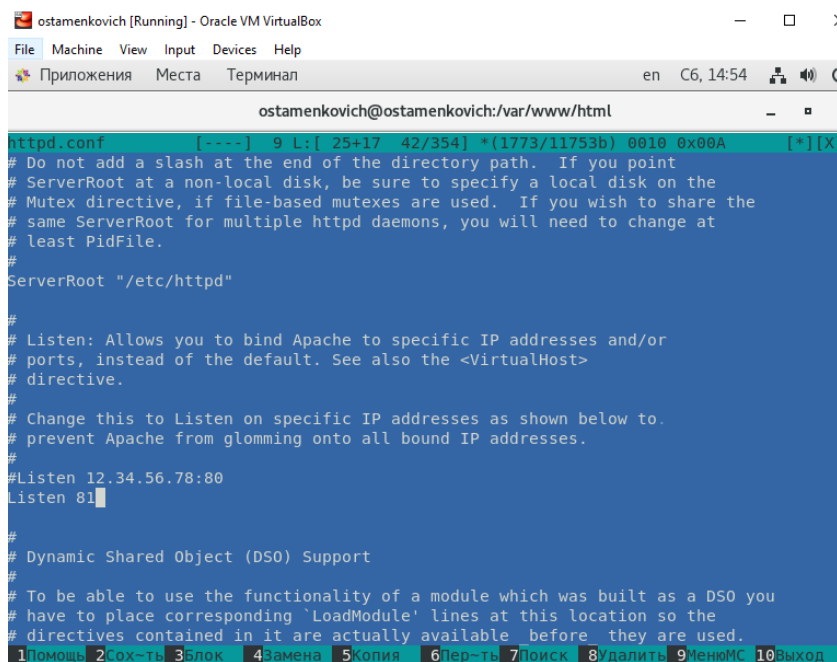
15. Проанализируйте ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? `ls -l /var/www/html/test.html` Просмотрите log-файлы веб-сервера Apache. Также просмотрите системный лог-файл: `tail /var/log/messages` Если в системе окажутся запущенными процессы `setroubleshootd` и `audtd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно.



```
ostamenkovich [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Приложения Места Терминал en C6, 14:53
ostamenkovich@ostamenkovich:/var/www/html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@ostamenkovich html]# chcon -t samba_share_t /var/www/html/test.html
[root@ostamenkovich html]# ls -Z /var/www/html/test.html
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[root@ostamenkovich html]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 5 окт 15 14:49 /var/www/html/test.html
[root@ostamenkovich html]# tail /var/log/messages
Oct 15 14:40:04 ostamenkovich systemd: Started Session 2 of user root.
Oct 15 14:40:04 ostamenkovich systemd: Removed slice User Slice of root.
Oct 15 14:48:32 ostamenkovich pulseaudio[2190]: [alsa-sink-Intel ICH] alsa-sink.c: ALSA woke us up to write new data to the device, but there was actually nothing to write.
Oct 15 14:48:32 ostamenkovich pulseaudio[2190]: [alsa-sink-Intel ICH] alsa-sink.c: Most likely this is a bug in the ALSA driver 'snd_intel8x0'. Please report this issue to the ALSA developers.
Oct 15 14:48:32 ostamenkovich pulseaudio[2190]: [alsa-sink-Intel ICH] alsa-sink.c: We were woken up with POLLOUT set -- however a subsequent snd_pcm_avail() returned 0 or another value < min_avail.
Oct 15 14:50:01 ostamenkovich systemd: Starting Cleanup of Temporary Directories...
Oct 15 14:50:01 ostamenkovich systemd: Created slice User Slice of root.
Oct 15 14:50:01 ostamenkovich systemd: Started Session 3 of user root.
Oct 15 14:50:01 ostamenkovich systemd: Started Cleanup of Temporary Directories.
Oct 15 14:50:01 ostamenkovich systemd: Removed slice User Slice of root.
[root@ostamenkovich html]# ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 5 окт 15 14:49 /var/www/html/test.html
[root@ostamenkovich html]#
```

Figure 2.6: лог ошибок

16. Попробуйте запустить веб-сервер Apache на прослушивание TCP-порта 81 (а не 80, как рекомендует IANA и прописано в /etc/services). Для этого в файле /etc/httpd/httpd.conf найдите строчку Listen 80 и замените её на Listen 81.



```
ostamenkovich [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Приложения Места Терминал en C6, 14:54
ostamenkovich@ostamenkovich:/var/www/html
httpd.conf [----] 9 L:[ 25+17 42/354] *(1773/11753b) 0010 0x00A [*][X]
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
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 specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#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.
```

Figure 2.7: переключение порта

17. Выполните перезапуск веб-сервера Apache. Произошёл сбой? Поясните почему? Сбой не происходит, порт 81 уже вписан в разрешенные
18. Проанализируйте лог-файлы: `tail -nl /var/log/messages` Просмотрите файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` и выясните, в каких файлах появились записи.
19. Выполните команду `semanage port -a -t http_port_t -p tcp 81` После этого проверьте список портов командой `semanage port -l | grep http_port_t` Убедитесь, что порт 81 появился в списке.
20. Попробуйте запустить веб-сервер Apache ещё раз.
21. Верните контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html`: `chcon -t httpd_sys_content_t /var/www/html/test.html` После этого попробуйте получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1:81/test.html`. Вы должны увидеть содержимое файла — слово «test».

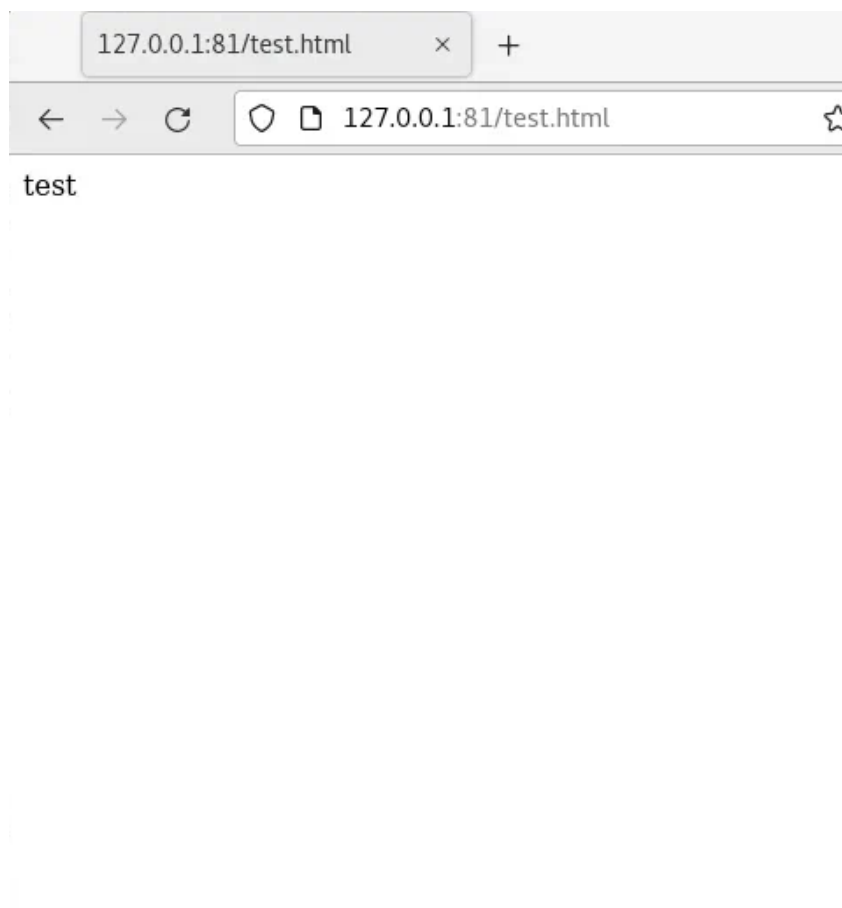


Figure 2.8: доступ по http на 81 порт

22. Исправьте обратно конфигурационный файл apache, вернув Listen 80.
23. Удалите привязку http\_port\_t к 81 порту: `semanage port -d -t http_port_t -p tcp 81` и проверьте, что порт 81 удалён.
24. Удалите файл `/var/www/html/test.html`: `rm /var/www/html/test.html`

## **3 Выводы**

В процессе выполнения лабораторной работы мною были получены базовые навыки работы с технологией seLinux.

# Список литературы

1. SELinux в CentOS
2. Веб-сервер Apache