

Отчёт по лабораторной работе №6

Мандатное разграничение прав в Linux

Жижченко Валерия Викторовна

Содержание

| | |
|--------------------------------------|---|
| Цель работы | 1 |
| Выполнение лабораторной работы | 1 |
| Вывод..... | 9 |

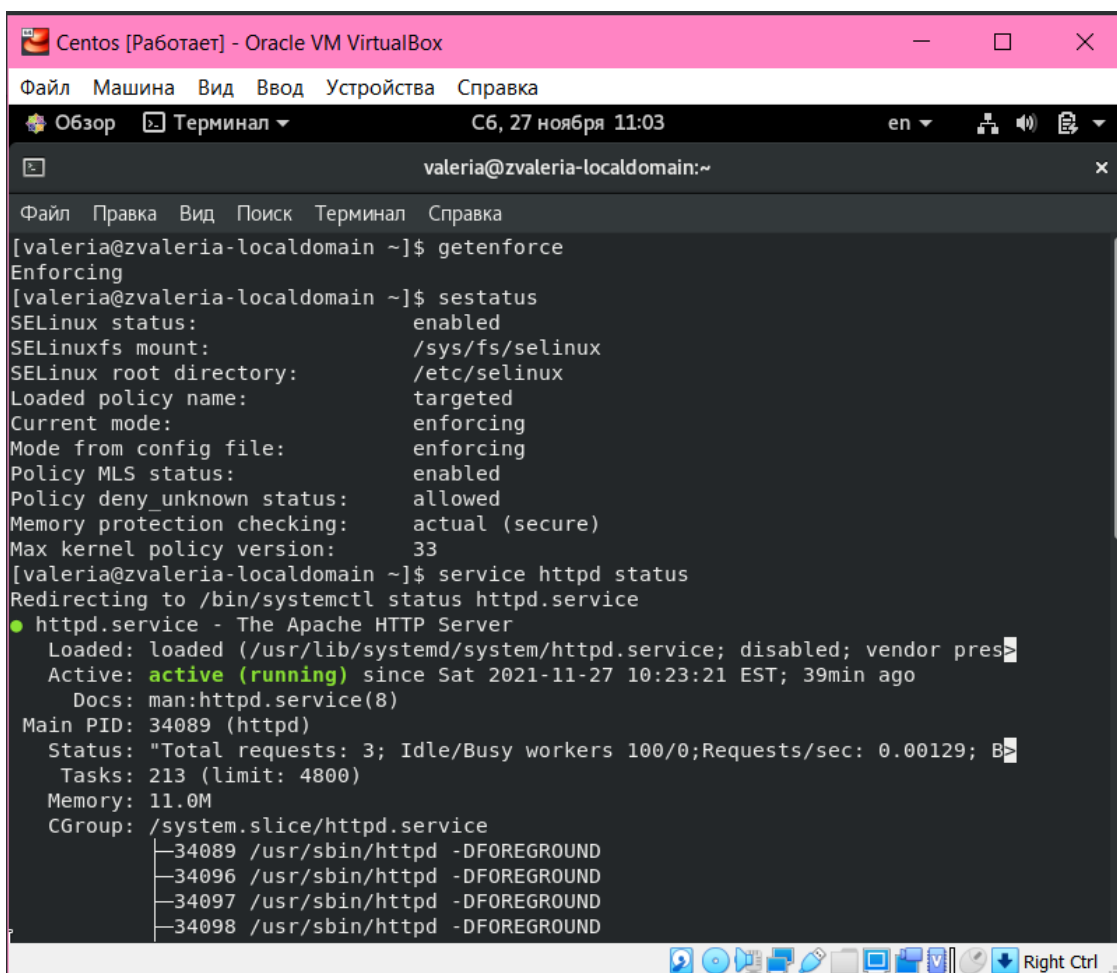
Цель работы

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

1. Вошли в систему с полученными учётными данными и убедились, что *SELinux* работает в режиме *enforcing* политики *targeted*:
\$ `sestatus`
2. Убедились, что веб-сервер работает:
\$ `service httpd status`



```
[valeria@zvaleria-localdomain ~]$ getenforce
Enforcing
[valeria@zvaleria-localdomain ~]$ 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
[valeria@zvaleria-localdomain ~]$ 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 pres>
   Active: active (running) since Sat 2021-11-27 10:23:21 EST; 39min ago
     Docs: man:httpd.service(8)
  Main PID: 34089 (httpd)
    Status: "Total requests: 3; Idle/Busy workers 100/0;Requests/sec: 0.00129; B>
      Tasks: 213 (limit: 4800)
     Memory: 11.0M
    CGroup: /system.slice/httpd.service
            └─34089 /usr/sbin/httpd -DFOREGROUND
              └─34096 /usr/sbin/httpd -DFOREGROUND
                └─34097 /usr/sbin/httpd -DFOREGROUND
                  └─34098 /usr/sbin/httpd -DFOREGROUND
```

Figure 1: Выполнение пунктов 1-2

3. Нашли веб-сервер *Apache* в списке процессов, определили его контекст безопасности:

```
$ ps -eZ | grep httpd
```

4. Посмотрели текущее состояние переключателей *SELinux* для *Apache*:

```
$ sestatus -b | grep httpd
```

The screenshot shows a terminal window titled "Centos [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

```
[valeria@zvaleria-localdomain ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0 root 34089 0.0 0.2 282904 1984 ? Ss 1
0:23 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34096 0.0 0.1 296784 1108 ? S 1
0:23 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34097 0.0 0.1 1485700 1340 ? Sl 1
0:23 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34098 0.0 0.1 1354572 1304 ? Sl 1
0:23 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 34099 0.0 0.1 1354572 1548 ? Sl 1
0:23 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 valeria 36214 0.0 0.1 12136 1156
pts/0 R+ 11:04 0:00 grep --color=auto httpd

[valeria@zvaleria-localdomain ~]$ 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
```

Figure 2: Выполнение пунктов 3-4

5. Посмотрели статистику по политике, также определили множество пользователей, ролей, типов:

\$ seinfo

```
[valeria@zvaleria-localdomain ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          31 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:      132      Permissions:      463
Sensitivities: 1      Categories:      1024
Types:        4958     Attributes:       255
Users:        8       Roles:           14
Booleans:     340     Cond. Expr.:     389
Allow:        112830   Neverallow:      0
Auditallow:   166     Dontaudit:       10362
Type_trans:   252747  Type_change:     87
Type_member:  35      Range_trans:     6015
Role allow:   37      Role_trans:      423
Constraints:  72      Validatetrans:   0
MLS Constran: 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:          33
Genfscon:     106    Portcon:         640
Netifcon:     0      Nodecon:         0

[valeria@zvaleria-localdomain ~]$
```

Figure 3: Вывод команды seinfo

6. Определили тип файлов и поддиректорий, находящихся в директории `/var/www`:

```
$ ls -lZ /var/www
```

7. Определили тип файлов, находящихся в директории `/var/www/html`:

```
$ ls -lZ /var/www/html
```

8. Определили что создание файлов в директории `/var/www/html` разрешено только пользователю `root`.

9. Создали от имени суперпользователя файл `/var/www/html/test.html`:

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

10. Проверили контекст созданного файла:

```
$ ls -Z /var/www/html/test.html
```

```
neticon: 0 nodecon: 0
[valeria@zvaleria-localdomain ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 11 23:58 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 23 ноя 27 10:45 html
[valeria@zvaleria-localdomain ~]$ ls -lZ /var/www/html
итого 4
-rw-r--r--. 1 root root unconfined_u:object_r:samba_share_t:s0 33 ноя 27 10:45 test.html
[valeria@zvaleria-localdomain ~]$ sudo vi /var/www/html/test.html
[sudo] пароль для valeria:
[valeria@zvaleria-localdomain ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[valeria@zvaleria-localdomain ~]$
```

Figure 4: Выполнение пунктов 6-10

11. Обратились к файлу через веб-сервер при помощи браузера:

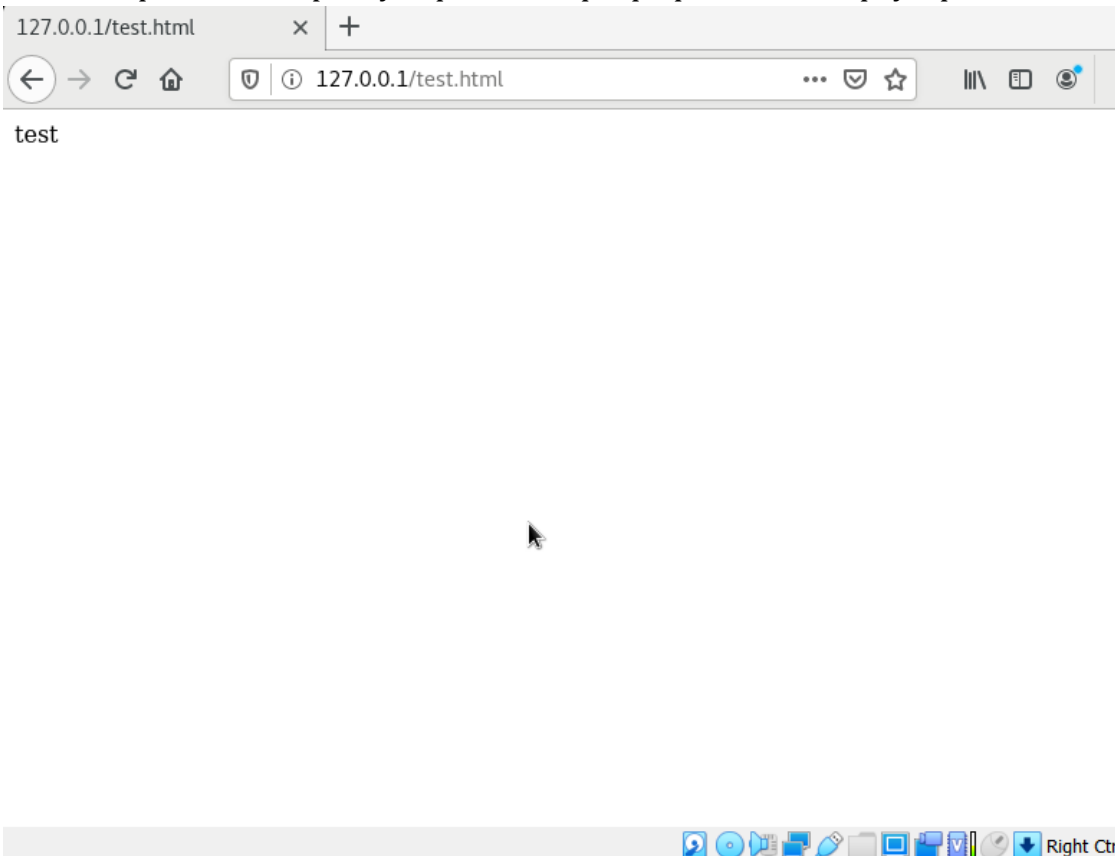


Figure 5: Файл test.html в браузере

12. Изучили справку `httpd_selinux` и выяснили, что для файлов `httpd` определены контексты `httpd_sys_content_t`, `httpd_sys_script_exec_t`, `httpd_sys_script_ro_t`, `httpd_sys_script_rw_t`, `httpd_sys_script_ra_t`, `httpd_unconfined_script_exec_t`.

Проверили контекст файла:

```
$ ls -Z /var/www/html/test.html
```

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
```



```
[valeria@zvaleria-localdomain ~]$ sudo chcon -t samba_share_t /var/www/html/test.html
[valeria@zvaleria-localdomain ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:samba_share_t:s0 /var/www/html/test.html
[valeria@zvaleria-localdomain ~]$
```

Figure 6: Выполнение пункта 13

14. Попробовали получить доступ к файлу через веб-сервер:

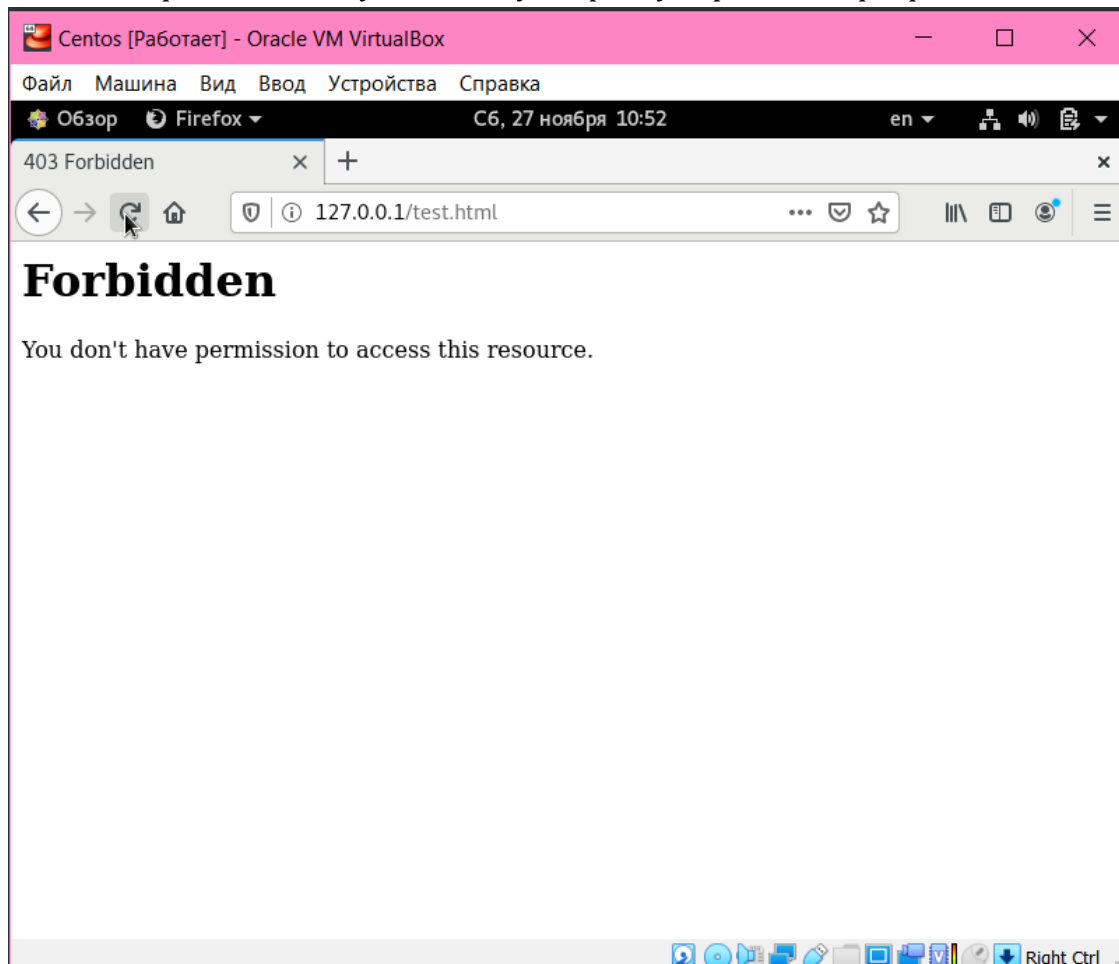


Figure 7: Попытка открыть файл `test.html` в браузере

15. Проанализировали почему файл не был отображён и посмотрели *log*-файлы веб-сервера *Apache*:

```
$ ls -l /var/www/html/test.html
$ tail /var/log/httpd/error_log
```

```
Centos [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Обзор Терминал C6, 27 ноября 11:26 en
valeria@zvaleria-localdomain:~
Файл Правка Вид Поиск Терминал Справка
[valeria@zvaleria-localdomain ~]$ ls -l /var/www/html/test.html
-rw-r--r--. 1 root root 33 ноя 27 10:45 /var/www/html/test.html
[valeria@zvaleria-localdomain ~]$ sudo tail /var/log/messages
Nov 27 11:03:20 zvaleria-localdomain journal[2744]: not GsPlugin error g-io-error-quark
:1: Ошибка при получении информации о файле «/home/valeria/.cache/gnome-software/shell-
extensions/gnome.json»: Нет такого файла или каталога
Nov 27 11:04:27 zvaleria-localdomain org.gnome.Shell.desktop[2266]: libinput error: eve
nt3 - ImExPS/2 Generic Explorer Mouse: client bug: event processing lagging behind by
14ms, your system is too slow
Nov 27 11:04:27 zvaleria-localdomain org.gnome.Shell.desktop[2266]: libinput error: eve
nt3 - ImExPS/2 Generic Explorer Mouse: client bug: event processing lagging behind by
24ms, your system is too slow
Nov 27 11:06:46 zvaleria-localdomain dbus-daemon[846]: [system] Activating via systemd:
service name='net.reactivated.Fprint' unit='fprintd.service' requested by ':1.553' (ui
d=0 pid=36281 comm="sudo vi /var/www/html/test.html " label="unconfined_u:unconfined_r:
unconfined_t:s0-s0:c0.c1023")
Nov 27 11:06:46 zvaleria-localdomain systemd[1]: Starting Fingerprint Authentication Dae
mon...
Nov 27 11:06:46 zvaleria-localdomain dbus-daemon[846]: [system] Successfully activated
service 'net.reactivated.Fprint'
Nov 27 11:06:46 zvaleria-localdomain systemd[1]: Started Fingerprint Authentication Dae
mon.
Nov 27 11:07:16 zvaleria-localdomain systemd[1]: fprintd.service: Succeeded.
Nov 27 11:09:53 zvaleria-localdomain org.gnome.Shell.desktop[2266]: Window manager warn
ing: last_user_time (4150735) is greater than comparison timestamp (4150723). This mos
t likely represents a buggy client sending inaccurate timestamps in messages such as _N
ET_ACTIVE_WINDOW. Trying to work around...
Nov 27 11:09:53 zvaleria-localdomain org.gnome.Shell.desktop[2266]: Window manager warn
```

Figure 8: Выполнение пункта 15

16. Изменили конфигурацию веб-сервера *Apache*, чтобы прослушивался порт 81.
17. Выполните перезапуск веб-сервера *Apache*. Так как все завершилось успешно, переходим в пункту 21.
18. Вернули контекст *httpd_sys_content_t* к файлу */var/www/html/test.html* и попробовали получить доступ к файлу через веб-сервер:

```
$ chcon -t httpd_sys_content_t /var/www/html/test.html
```

```
[valeria@zvaleria-localdomain ~]$ sudo vi /etc/httpd/conf/httpd.conf
[valeria@zvaleria-localdomain ~]$ sudo systemctl restart httpd
[valeria@zvaleria-localdomain ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Sat 2021-11-27 11:21:11 EST; 19s ago
     Docs: man:httpd.service(8)
  Main PID: 36794 (httpd)
    Status: "Started, listening on: port 81"
     Tasks: 213 (limit: 4800)
    Memory: 22.4M
    CGroup: /system.slice/httpd.service
            └─36794 /usr/sbin/httpd -DFOREGROUND
              └─36802 /usr/sbin/httpd -DFOREGROUND
                └─36803 /usr/sbin/httpd -DFOREGROUND
                  └─36804 /usr/sbin/httpd -DFOREGROUND
                    └─36805 /usr/sbin/httpd -DFOREGROUND

ноя 27 11:21:11 zvaleria-localdomain systemd[1]: Starting The Apache HTTP Server...
ноя 27 11:21:11 zvaleria-localdomain httpd[36794]: AH00558: httpd: Could not reliably
ноя 27 11:21:11 zvaleria-localdomain systemd[1]: Started The Apache HTTP Server.
ноя 27 11:21:26 zvaleria-localdomain httpd[36794]: Server configured, listening on: po
[valeria@zvaleria-localdomain ~]$
```

Figure 9: Выполнение пунктов 16-21

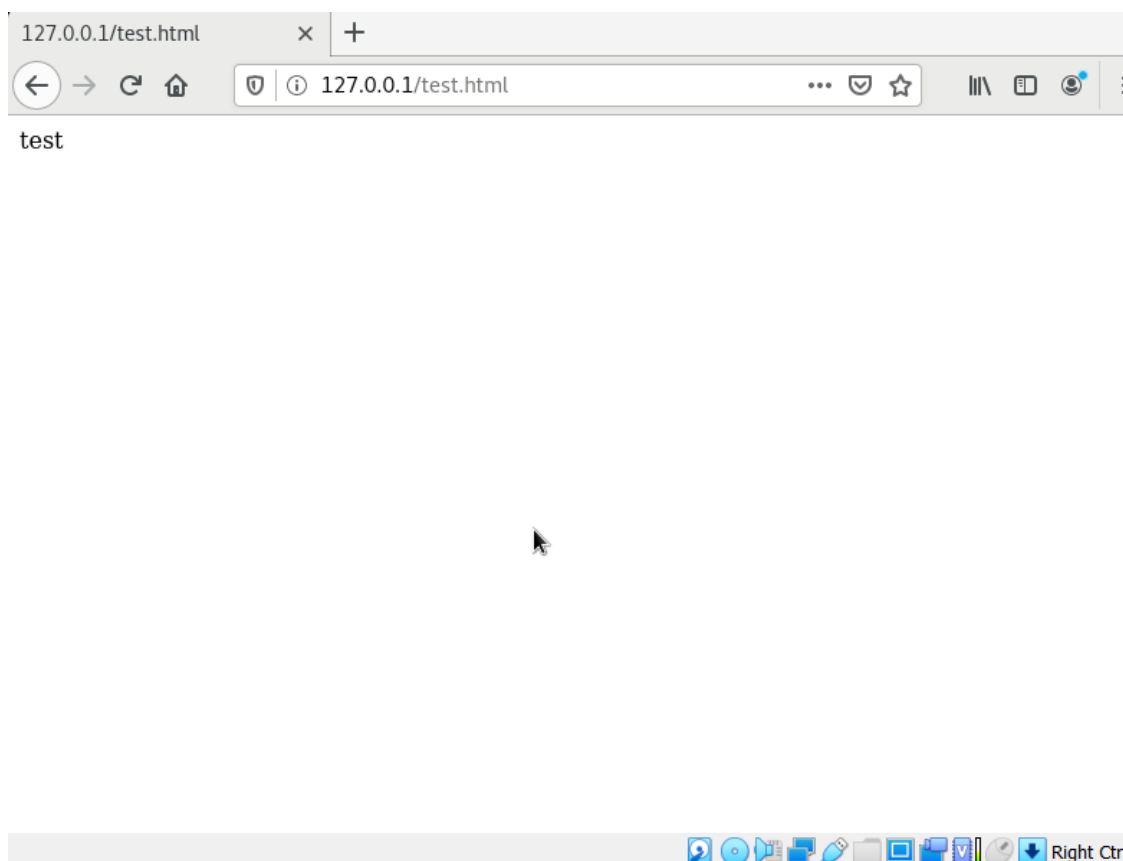


Figure 10: Файл test.html в браузере через 81 порт

22. Исправили обратно конфигурационный файл *apache*, вернув *Listen 80*.
23. Удалили файл */var/www/html/test.html*:


```
$ rm /var/www/html/test.html
```

```
[valeria@zvaleria-localdomain ~]$ vi /etc/h  
host.conf hostname hosts hp/ httpd/  
[valeria@zvaleria-localdomain ~]$ vi /etc/httpd/httpd.conf  
[valeria@zvaleria-localdomain ~]$ sudo chcon -t httpd_sys_content_t /var/www/html/test  
.html  
[valeria@zvaleria-localdomain ~]$ rm /var/www/html/test.html  
rm: удалить защищенный от записи обычный файл '/var/www/html/test.html'?
```

Figure 11: Файл test.html удален

Вывод

Развили навыки администрирования ОС Linux. Получили первое практическое знакомство с технологией SELinux. Проверили работу SELinx на практике совместно с веб-сервером Apache.