Лабораторная работа №6

Мандатное разграничение прав в Linux

Выполнила: Пономарева Лилия Михайловна
НПИбд-02-19

Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux1. Проверить работу SELinux на практике совместно с веб-сервером Apache.

Убедилась, что SELinux работает в режиме enforcing политики targeted

```
[lmponomareva@lmponomareva ~]$ getenforce
Enforcing
[lmponomareva@lmponomareva ~]$ 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
```

Запустила веб-сервер

```
[lmponomareva@lmponomareva ~]$ service httpd start
Redirecting to /bin/systemctl start httpd.service
[lmponomareva@lmponomareva ~]$ 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 pr>
     Active: active (running) since Sat 2022-10-15 09:54:43 MSK; 3s ago
       Docs: man:httpd.service(8)
   Main PID: 39855 (httpd)
     Status: "Started, listening on: port 80"
```

Нашла веб-сервер Apache в списке процессов

```
[lmponomareva@lmponomareva ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0    root       39855  0.2  0.5  20064 11596 ?
 Ss   09:54   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     39863  0.0  0.3  21516  7284 ?
 S    09:54   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     39864  0.0  0.9 1210352 19156 ?
 Sl   09:54   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     39867  0.0  0.8 1079216 17108 ?
 Sl   09:54   0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0    apache     39872  0.0  0.8 1079216 17108 ?
 Sl   09:54   0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 lmponom+ 40111 0.0  0.1 22
1668 2340 pts/1 S+ 09:55   0:00 grep --color=auto httpd
```

Текущее состояние переключателей SELinux для Apache

```
[lmponomareva@lmponomareva ~]$ 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
```

Статистика по политике

```
[lmponomareva@lmponomareva ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:             33 (MLS enabled)
Target Policy:              selinux
Handle unknown classes:     allow
  Classes:              133    Permissions:          454
  Sensitivities:          1    Categories:          1024
  Types:               5002    Attributes:           254
  Users:                  8    Roles:                 14
  Booleans:             347    Cond. Expr.:          381
  Allow:              63996    Neverallow:             0
  Auditallow:           168    Dontaudit:           8417
  Type_trans:        258486    Type_change:           87
  Type_member:           35    Range_trans:         5960
```

Тип поддиректорий в директории /var/www

```
[lmponomareva@lmponomareva ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 May 16 15:10 html
```

Круг пользователей с разрешением на создание файлов в /var/www/html

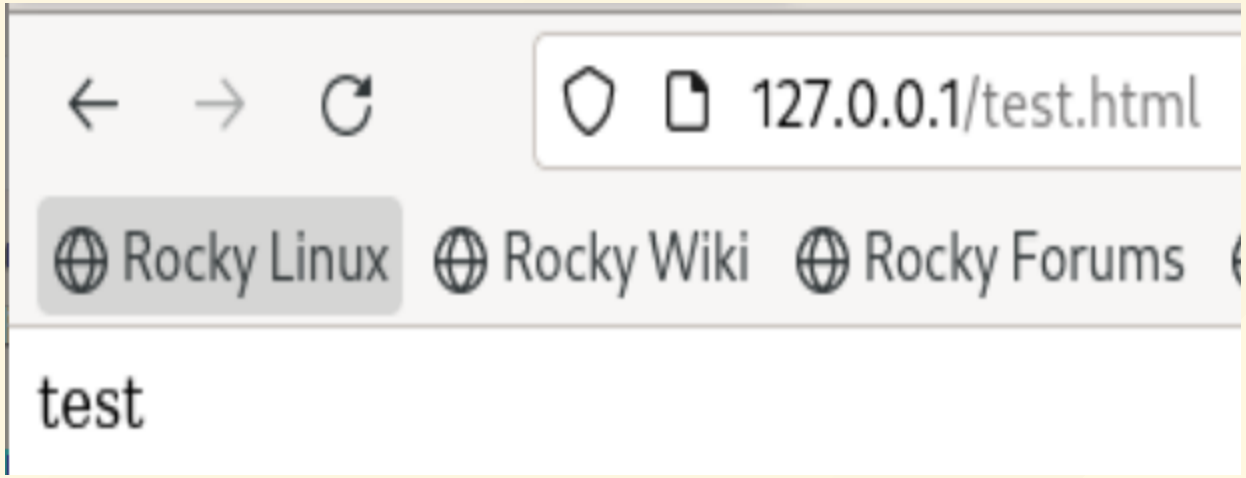
```
[lmponomareva@lmponomareva ~]$ ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 May 16 15:10 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0     6 May 16 15:10 html
```

Создала html-файл /var/www/html/test.html

Проверила контекст созданного файла

```
[lmponomareva@lmponomareva ~]$ ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
```

Обратилась к файлу через веб-сервер



Man httpd_selinux

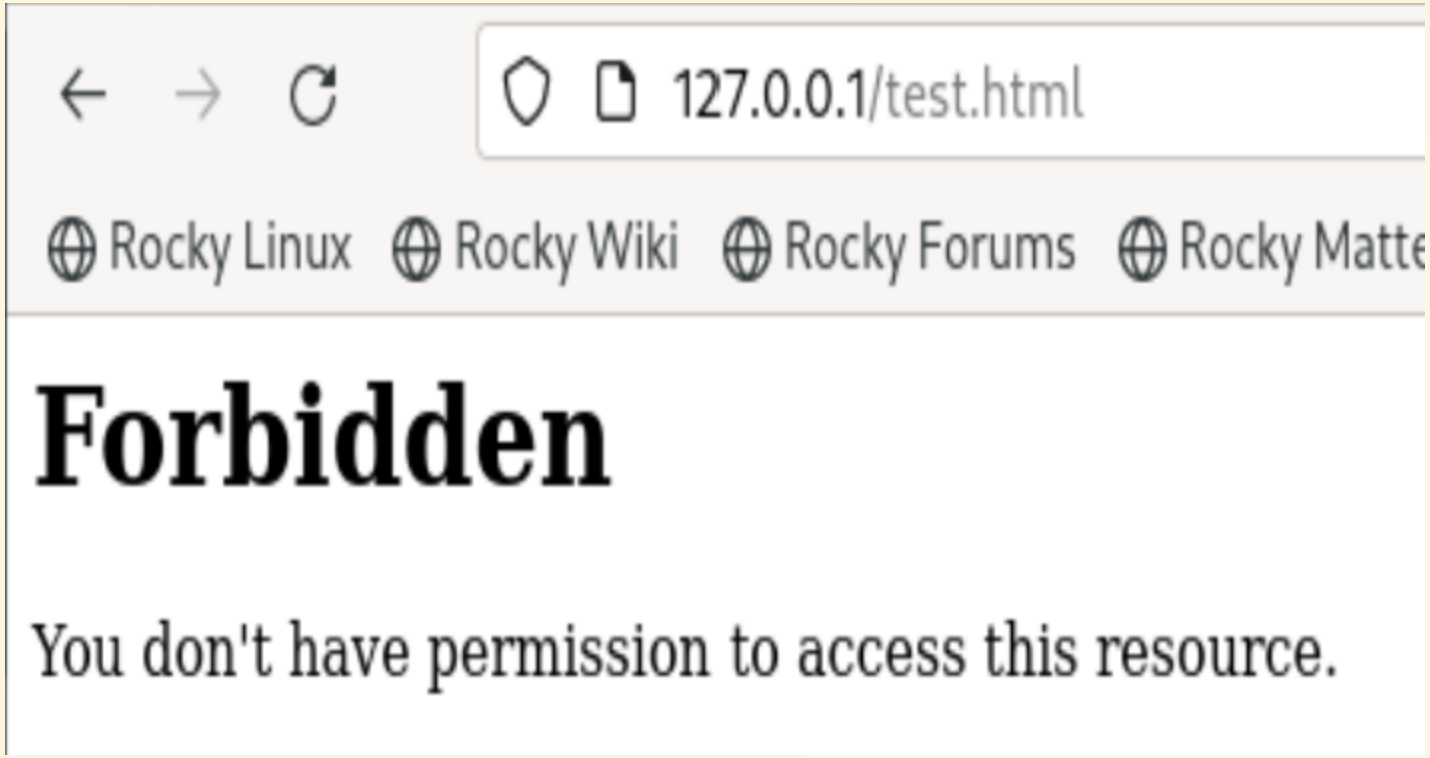
```
httpd_sys_rw_content_t

      /etc/glpi(/.*)?
      /etc/horde(/.*)?
      /etc/drupal.*
      /etc/z-push(/.*)?
      /var/lib/svn(/.*)?
      /var/www/svn(/.*)?
      /etc/owncloud(/.*)?
      /var/www/html(/.*)?/uploads(/.*)?
      /var/www/html(/.*)?/wp-content(/.*)?
      /var/www/html(/.*)?/sites/default/files(/.*)?
      /var/www/html(/.*)?/sites/default/settings.php
      /etc/mock/koji(/.*)?
      /var/lib/drupal.*
      /etc/zabbix/web(/.*)?
      /var/log/z-push(/.*)?
```

Изменила контекст файла /var/www/html/test.html

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

Обратилась к файлу через веб-сервер



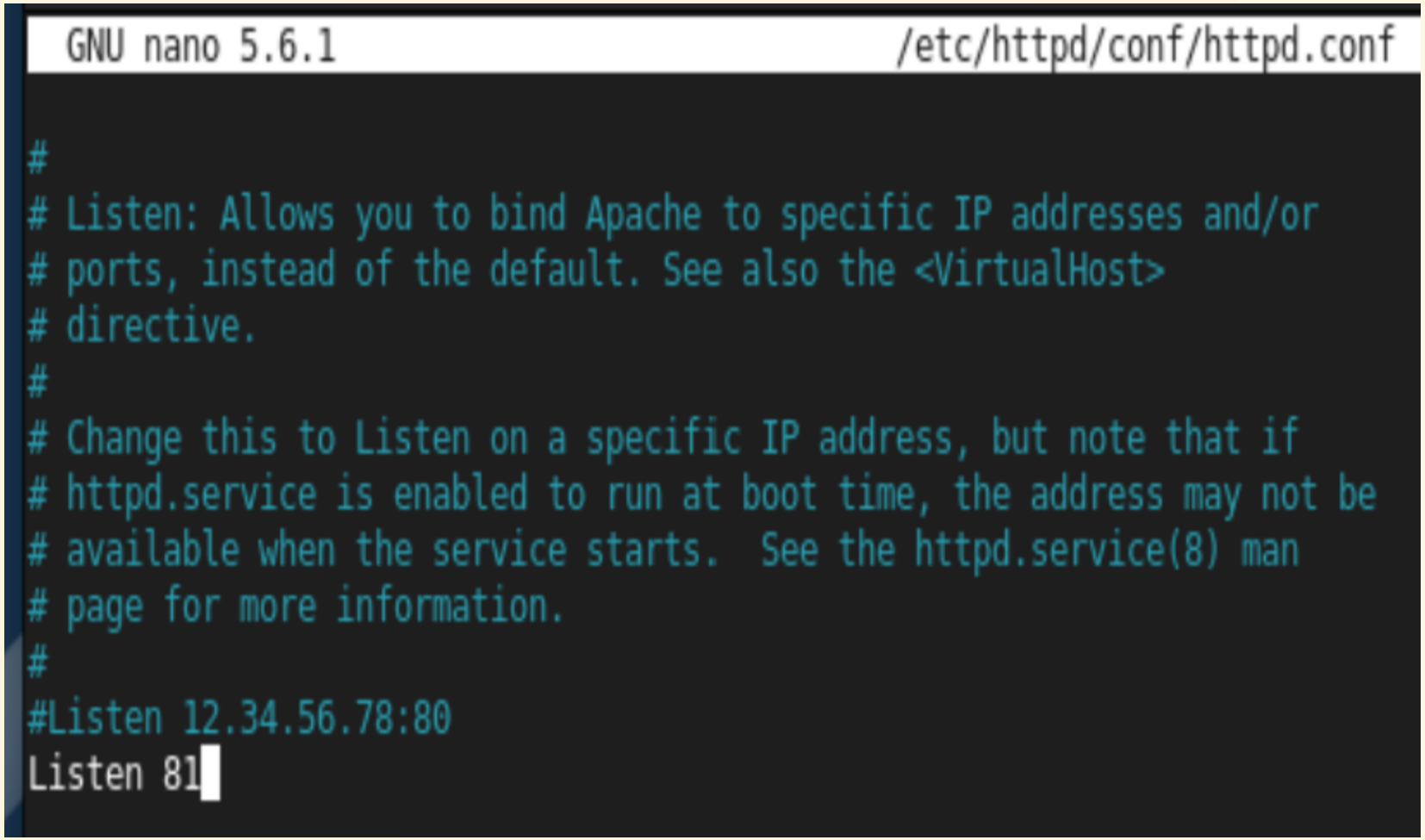
Log-файлы веб-сервера Apache

```
[root@lmponomareva lmponomareva]# tail /var/log/audit/audit.log
type=AVC msg=audit(1665822914.169:322): avc:  denied  { getattr } for  pid=39872 comm="httpd" path="/var/www
tml/test.html" dev="dm-0" ino=101177494 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r
amba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1665822914.169:322): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=7f3
4004ff0 a2=7f3b6883f830 a3=0 items=0 ppid=39855 pid=39872 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsui
48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:syste
r:httpd_t:s0 key=(null)ARCH=x86_64 SYSCALL=newfstatat AUID="unset" UID="apache" GID="apache" EUID="apache" S
D="apache" FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1665822914.169:322): proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F55
44
type=AVC msg=audit(1665822914.169:323): avc:  denied  { getattr } for  pid=39872 comm="httpd" path="/var/www
tml/test.html" dev="dm-0" ino=101177494 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r
amba_share_t:s0 tclass=file permissive=0
type=SYSCALL msg=audit(1665822914.169:323): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=7f3
4007140 a2=7f3b6883f830 a3=100 items=0 ppid=39855 pid=39872 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fs
d=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:sys
```

Посмотрела системный лог-файл

```
Oct 15 11:35:21 lmponomareva setroubleshoot[42230]: SELinux is preventing /usr/sbin/httpd from getattr acces
on the file /var/www/html/test.html.#012#012*****  Plugin restorecon (92.2 confidence) suggests   **********
**********#012#012If you want to fix the label. #012/var/www/html/test.html default label should be httpd_
s_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to insufficient pe
issions to access a parent directory in which case try to change the following command accordingly.#012Do#01
 /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
bel on test.html to public_content_t or public_content_rw_t.#012Do#012# semanage fcontext -a -t public_conte
_t '/var/www/html/test.html'#012# restorecon -v '/var/www/html/test.html'#012#012*****  Plugin catchall (1.4
confidence) suggests   **********#012#012If you believe that httpd should be allowed getattr
ccess on the test.html file by default.#012Then you should report this as a bug.#012You can generate a local
olicy module to allow this access.#012Do#012allow this access for now by executing:#012# ausearch -c 'httpd'
-raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
```

Запустила веб-сервер Apache на прослушивание TCP-порта 81



Добавила порт 81 в список портов

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

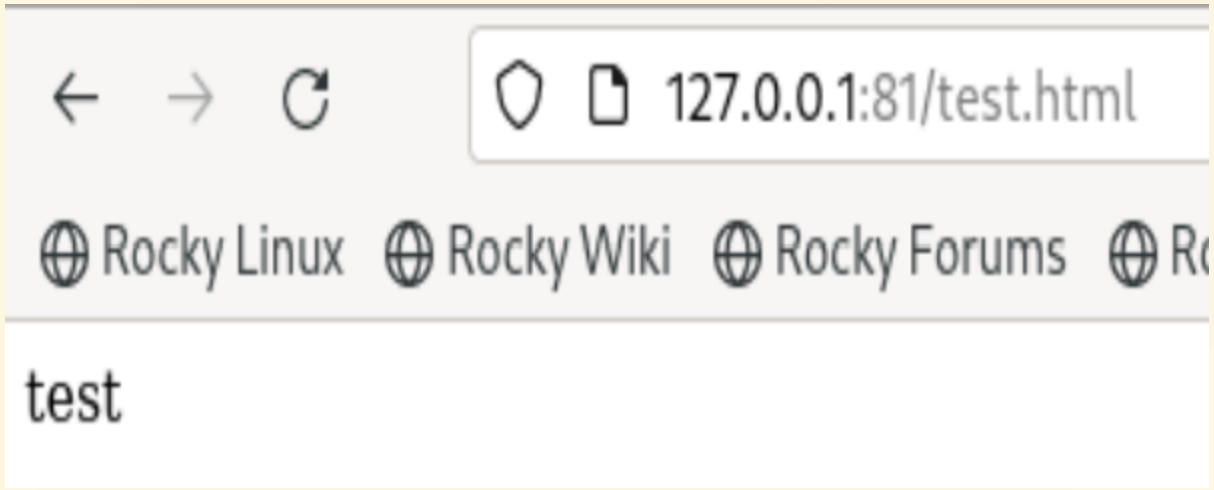
Перезапустила Apache

```
[root@lmponomareva lmponomareva]# semanage port -l | gre
http_port_t                    tcp      80, 81, 443, 488
pegasus_http_port_t            tcp      5988
[root@lmponomareva lmponomareva]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
```

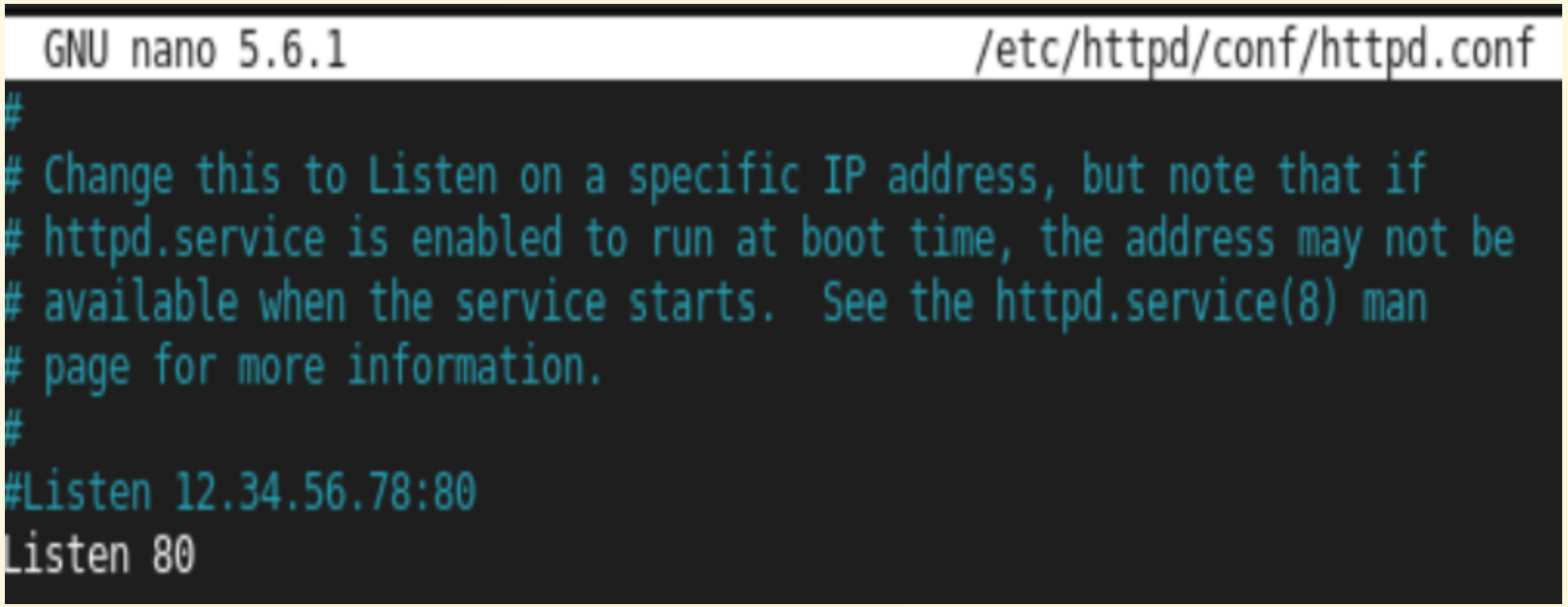
Вернула контекст httpd_sys_content__t

```
[root@lmponomareva lmponomareva]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@lmponomareva lmponomareva]#
```

Обратилась к файлу через веб-сервер



Исправила конфигурационный файл apache



Попробовала удалить привязку http_port_t к 81 порту

```
[root@lmponomareva lmponomareva]# semanage port -d -t http_port_t -p tcp 81
ValueError: Port tcp/81 is defined in policy, cannot be deleted
[root@lmponomareva lmponomareva]#
```

Удалила файл /var/www/html/test.html

```
[root@lmponomareva lmponomareva]# rm /var/www/html/test.html
rm: remove regular file '/var/www/html/test.html'? y
[root@lmponomareva lmponomareva]#
```

Вывод

Получили практическое знакомство с технологией SELinux1. Проверили работу SELinx на практике совместно с веб-сервером Apache.