

# Знакомство с SELinux

---

Савченко Елизавета НБИ-01-20

14 октября, 2023, Москва, Россия

Российский Университет Дружбы Народов

# Цели и задачи

---

SELinux или Security Enhanced Linux — это улучшенный механизм управления доступом, разработанный Агентством национальной безопасности США (АНБ США) для предотвращения злонамеренных вторжений. Он реализует принудительную (или мандатную) модель управления доступом (англ. Mandatory Access Control, MAC) поверх существующей дискреционной (или избирательной) модели (англ. Discretionary Access Control, DAC), то есть разрешений на чтение, запись, выполнение.

Apache – это свободное программное обеспечение для размещения веб-сервера. Он хорошо показывает себя в работе с масштабными проектами, поэтому заслуженно считается одним из самых популярных веб-серверов. Кроме того, Apache очень гибок в плане настройки, что даёт возможность реализовать все особенности размещаемого веб-ресурса.

## Цель лабораторной 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**

---

# Запуск HTTP-сервера

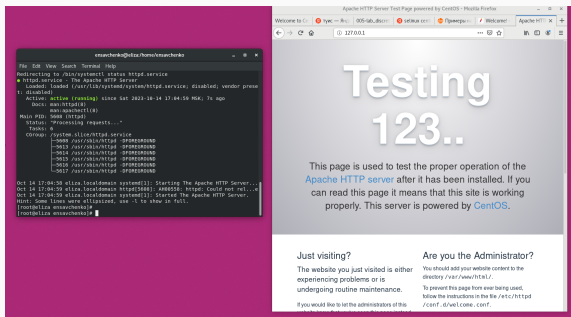
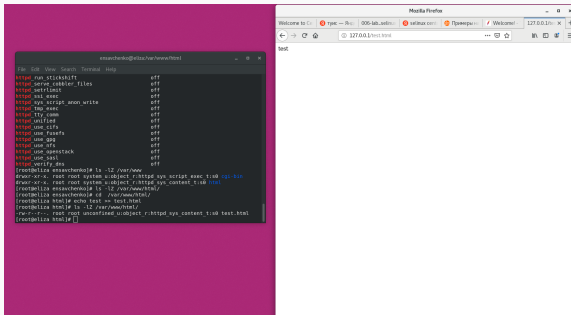


Figure 1: запуск http

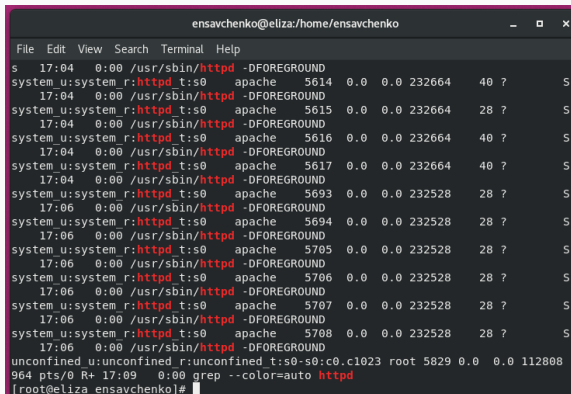
## Создание HTML-файла



### Figure 2: создание html-файла и доступ по http



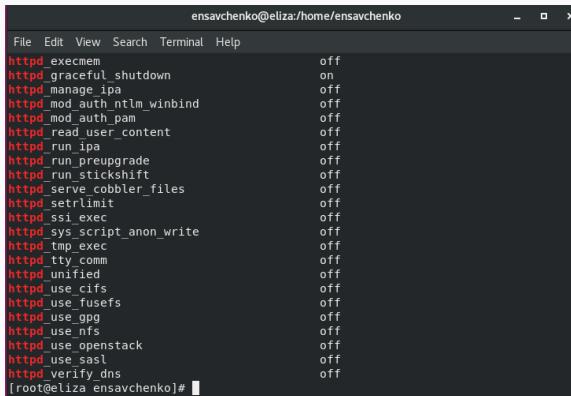
# Контекст безопасности http



```
ensavchenko@eliza:/home/ensavchenko
File Edit View Search Terminal Help
s 17:04 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 5614 0.0 0.0 232664 40 ? S
17:04 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 5615 0.0 0.0 232664 28 ? S
17:04 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 5616 0.0 0.0 232664 40 ? S
17:04 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 5617 0.0 0.0 232664 40 ? S
17:04 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 5693 0.0 0.0 232528 28 ? S
17:06 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 5694 0.0 0.0 232528 28 ? S
17:06 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 5705 0.0 0.0 232528 28 ? S
17:06 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 5706 0.0 0.0 232528 28 ? S
17:06 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 5707 0.0 0.0 232528 28 ? S
17:06 0:00 /usr/sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0 apache 5708 0.0 0.0 232528 28 ? S
17:06 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 root 5829 0.0 0.0 112808
964 pts/0 R+ 17:09 0:00 grep --color=auto httpd
[root@eliza ensavchenko]#
```

Figure 3: Контекст безопасности http

# Переключатели SELinux для http

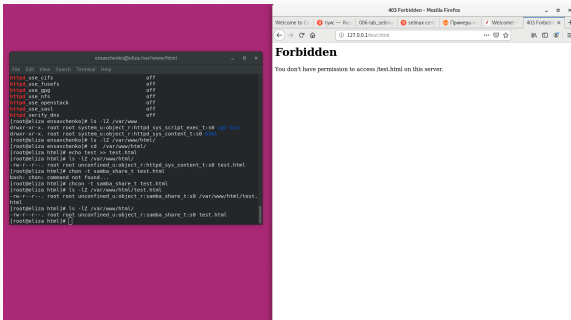
A terminal window titled 'ensavchenko@eliza:/home/ensavchenko' with standard window controls. The terminal shows a list of SELinux configuration options for httpd, each followed by its current status. The options are: httpd\_execmem (off), httpd\_graceful\_shutdown (on), httpd\_manage\_ipa (off), httpd\_mod\_auth\_ntlm\_winbind (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), and httpd\_verify\_dns (off). The prompt at the bottom is '[root@eliza ensavchenko]#'.

```
ensavchenko@eliza:/home/ensavchenko
File Edit View Search Terminal Help
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
[root@eliza ensavchenko]#
```

**Figure 4:** переключатели SELinux для http



## Ошибка доступа после изменения контекста

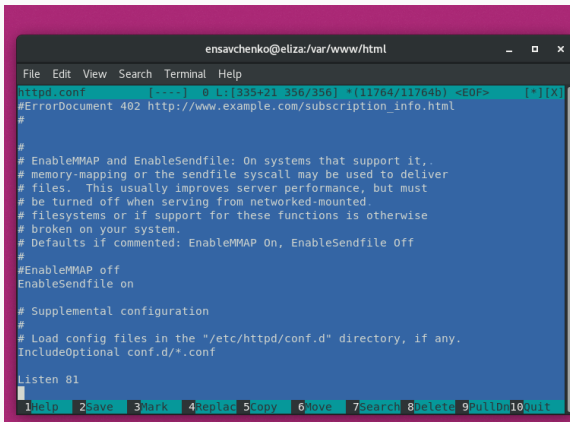


**Figure 6:** ошибка доступа после изменения контекста

```
[root@eliza html]# tail /var/log/messages
Oct 14 17:14:10 eliza setroubleshoot: failed to retrieve rpm info for /var/www/html/test.html
Oct 14 17:14:10 eliza setroubleshoot: SELinux is preventing /usr/sbin/httpd from
getattr access on the file /var/www/html/test.html. For complete SELinux messages run:
sealert -l f167e3aa-e038-479e-9b4e-38ca39627967
Oct 14 17:14:10 eliza python: SELinux is preventing /usr/sbin/httpd from getattr
access 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_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.#012Do#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.#012Do#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 getattr 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.#012Do#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 17:14:15 eliza setroubleshoot: failed to retrieve rpm info for /var/www/html
```

Figure 7: лог ошибок

# Переключение порта



```
ensavchenko@eliza:var/www/html
File Edit View Search Terminal Help
httpd.conf  [---] 0 L:[335+21 356/356] *(11764/11764b) <EOF>  [*][X]
#ErrorDocument 402 http://www.example.com/subscription_info.html
#
#
# EnableMMAP and EnableSendfile: On systems that support it,.
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
EnableSendfile on
# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
Listen 81
1Help 2Save 3Mark 4replac 5copy 6love 7Search 8Delete 9PullDn 10Quit
```

**Figure 8:** переключение порта

## Доступ по http на 81 порт

```

Oct 14 17:14:15 eliza setroubleshot: failed to retrieve rpm info for /var/www/html/test.html
Oct 14 17:14:17 eliza setroubleshot: SELinux is preventing /usr/sbin/httpd from getting access on the file /var/www/html/test.html. For complete SELinux messages run: sealert -l f167e3aa-0398-479e-9b4c-38ca39627967
Oct 14 17:14:17 eliza python: SELinux is preventing /usr/sbin/httpd from getting access on the file /var/www/html/test.html?***** Plugin restorecon (92.2 confidence) suggests *****
#12You can try to change the label so that httpd would be allowed to get access. You can do this with a command like: restorecon -v /var/www/html/test.html?***** Plugin public_content_t (7.83 confidence) suggests *****
#12You can try to change the label on test.html to public content t or public content_t?***** Plugin fcontext -a -t public content_t /var/www/html/test.html?***** Plugin restorecon -v /var/www/html/test.html?***** Plugin catchall (1.41 confidence) suggests *****
#12You can try to change the label on test.html to public content t or public content_t?***** Plugin httpd should be allowed to get access on the test.html file by default.
#12Then you should report this as a bug.
#12You can generate a local policy module to allow this access.
#12Below is how this access can be now by executing:
#12$ sudo ausearch -c 'httpd' --raw | audit2allow -M my-httpd?*****
#12$ sudo semodule -i my-httpd.pp?*****
Oct 14 17:14:36 eliza dbus[649]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service'
Oct 14 17:14:36 eliza systemd: Starting Hostname Service...
Oct 14 17:14:36 eliza dbus[649]: [system] Successfully activated service 'org.freedesktop.hostname1'
Oct 14 17:14:36 eliza systemd: Started Hostname Service.
[root@eliza html]# mcedit /etc/httpd/conf/httpd.conf
[root@eliza html]# mcedit /etc/httpd/conf/httpd.conf
[root@eliza html]# mcedit /etc/httpd/conf/httpd.conf
[root@eliza html]# mcedit /etc/httpd/conf/httpd.conf
[root@eliza html]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@eliza html]# semanage port -a -t httpd_port -t tcp B1
ERROR: could not find datum for type httpd port
ValueError: Type httpd port is invalid, must be a port type
[root@eliza html]# semanage port -l | grep http_post_t
[root@eliza html]# chcon -t httpd_sys_content_t test.html
[root@eliza html]# ls -lZ test.html
-rw-r--r-- 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@eliza html]#

```

### Figure 9: доступ по http на 81 порт

## **Выводы**

---



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