

# Знакомство с SELinux

---

Тихонова Екатерина

9 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

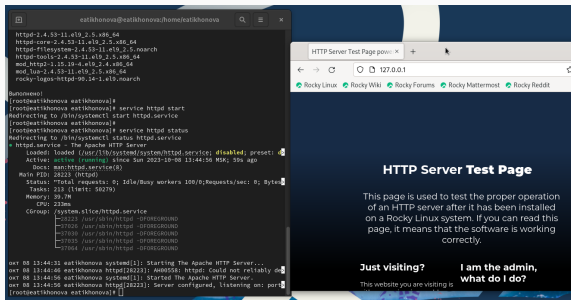
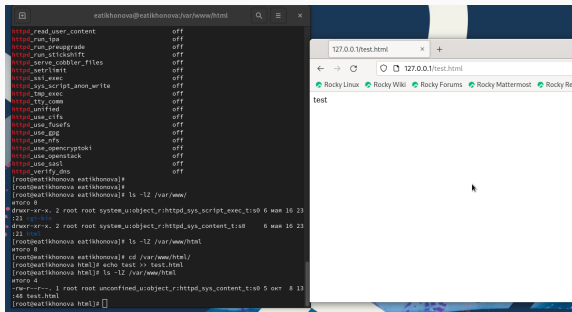


Figure 1: запуск http

# Создание HTML-файла



The image shows a terminal window on the left and a web browser window on the right. The terminal window displays the configuration of various services, all of which are set to 'off'. It then shows the user navigating to the directory `/var/www/html` and creating a file named `test.html` with the content `test`. The web browser window on the right shows the URL `127.0.0.1/test.html` and displays the content `test`.

```
eatikhonova@eatikhonova: /var/www/html
httpd_read_user_content off
httpd_run_ipa off
httpd_run_preupgrade off
httpd_run_stickshft off
httpd_serve_cobbler_files off
httpd_setristmt off
httpd_sasl_exec off
httpd_sys_script_anon_write off
httpd_top_exec off
httpd_tty_com off
httpd_untified off
httpd_use_clfs off
httpd_use_fusefs off
httpd_use_gpg off
httpd_use_nfs off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_sasl off
httpd_verify_doc off
[root@eatikhonova eatikhonova]#
[root@eatikhonova eatikhonova]#
[root@eatikhonova eatikhonova]# ls -l /var/www/
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23
-rw-r--r--. 1 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23
-rw-r--r--. 1 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23
[root@eatikhonova eatikhonova]# cd /var/www/html
[root@eatikhonova eatikhonova]# echo test > test.html
[root@eatikhonova eatikhonova]# ls -l /var/www/html
total 0
-rw-r--r--. 1 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23
-rw-r--r--. 1 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23
-rw-r--r--. 1 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23
-rw-r--r--. 1 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23
[root@eatikhonova eatikhonova]#
```

Figure 2: создание html-файла и доступ по http



# Изменение контекста безопасности

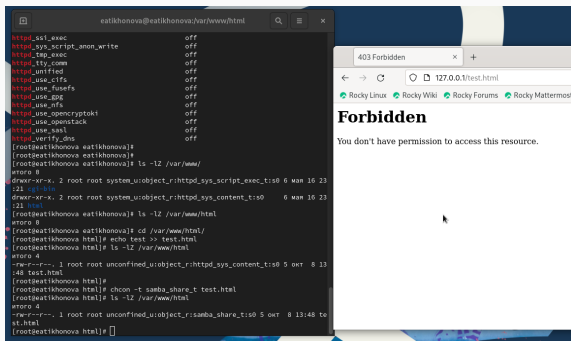
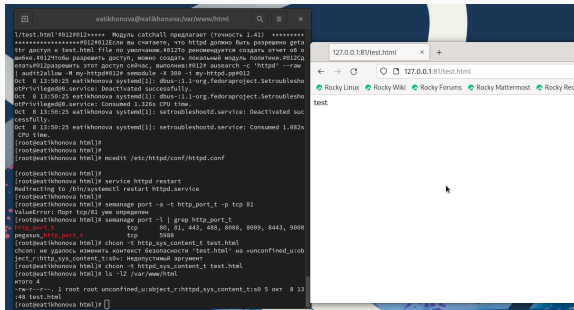


Figure 3: ошибка доступа после изменения контекста

# Переключение порта и восстановление контекста безопасности



The image shows a terminal window on the left and a web browser on the right. The terminal window is running a series of commands to configure and restart the HTTP service. The browser window shows the URL 127.0.0.1:81/test.html, indicating a successful connection to the service on port 81.

```
1/test.html#012P012***** Mugsy catchall pdeanarar (ромность 1.41) *****
*****#0124012Смн вы считаете, что httpd должно быть безопасно gets
tcp доступ к test.html file по умолчанию.#012То рекомендуется создать строк 06 0
wdev.#012Итого разрабарт доступ, можно создать локальный модуль политики.#012Сд
еать#012запустить этот доступ ссдкк, выполнено:#012 аусреш -с 'httpd' --row
| audit2allow -M my-httpd#012 smodule -X 300 -i my-httpd.pp#012
Oct 8 13:50:25 eatikhonova systemd[1]: dbus-1.1-0.org.fedoraproject.Setroublesho
oPrivilege@0.service: Deactivated successfully.
Oct 8 13:50:25 eatikhonova systemd[1]: dbus-1.1-0.org.fedoraproject.Setroublesho
oPrivilege@0.service: Consumed 1.120s CPU time.
Oct 8 13:50:25 eatikhonova systemd[1]: setroubleshootd.service: Deactivated suc
cessfully.
Oct 8 13:50:25 eatikhonova systemd[1]: setroubleshootd.service: Consumed 1.082s
CPU time.
[root@eatikhonova html]#
[root@eatikhonova html]#
[root@eatikhonova html]# mcedit /etc/httpd/conf/httpd.conf
[root@eatikhonova html]#
[root@eatikhonova html]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@eatikhonova html]#
[root@eatikhonova html]# semanage port -a -t http_port_t -p tcp 81
ValueError: Mapr tcp/81 yw onpagehem
[root@eatikhonova html]# semanage port -l | grep http_port_t
http_port_t tcp 80, 81, 443, 450, 8000, 8009, 8443, 9000
pegasus_http_port_t tcp 5088
[root@eatikhonova html]# chcon -t http_sys_content_t test.html
chcon: не удалось изменить контекст безопасности 'test.html' на 'unconfined_u:obj
ect_r:http_sys_content_t:s0': неопытные аргументы
[root@eatikhonova html]# chcon -t http_sys_content_t test.html
[root@eatikhonova html]# ls -ls /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:http_sys_content_t:s0 5 окр 8 13
-00 test.html
[root@eatikhonova html]#
```

Figure 4: доступ по http на 81 порт

## **Выводы**

---

## Результаты выполнения лабораторной работы

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