

# Знакомство с SELinux

---

Андриевская Анастасия

27 сентября, 2024, 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

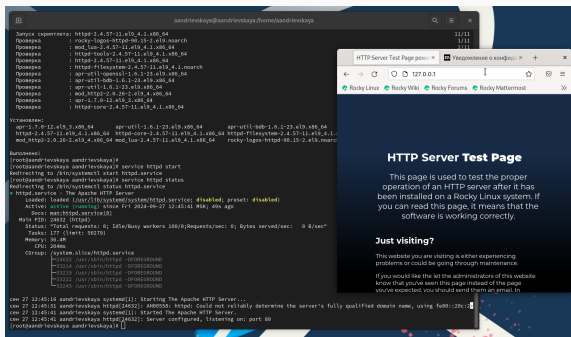


Figure 1: запуск http

# Создание HTML-файла

```
httd_data_audit off
httd_dbus_ssd off
httd_dontaudit_search_dirs off
httd_enable_apt on
httd_enable_ftp_server off
httd_enable_homedirs off
httd_enable_udev off
httd_graceful_shutdown off
httd_hmnpkg_1pa off
httd_md_auth_otp_wirbind off
httd_md_auth_otp off
httd_read_user_content off
httd_run_1pa off
httd_run_upgrade off
httd_run_activex off
httd_serv_cooler_files off
httd_user_taint off
httd_ssl_key off
httd_sys_script_asec_write off
httd_tap_exec off
httd_tty_console off
httd_unified off
httd_uxa_cifs off
httd_uxa_fusefs off
httd_uxa_dsp off
httd_uxa_off off
httd_uxa_opencryptoki off
httd_uxa_openssl off
httd_uxa_saml off
httd_verify_dns off
[rookie@andrievskaya sander-levskaya]$
[rookie@andrievskaya sander-levskaya]$
[rookie@andrievskaya sander-levskaya]$
[rookie@andrievskaya sander-levskaya]$ ls -l /var/www/
total 8
drwxr-xr-x. 2 root root system:object_r/httpd_sys_content_t:0 4 ser  8 19:38 cgi-bin
drwxr-xr-x. 2 root root system:object_r/httpd_sys_content_t:0e 4 ser  8 19:39 html
[rookie@andrievskaya sander-levskaya]$ ls -l /var/www/html/
total 8
[rookie@andrievskaya sander-levskaya]$ cd /var/www/html/
[rookie@andrievskaya html]$ echo test > test.html
[rookie@andrievskaya html]$ ls -l /var/www/html/
total 4
-rw-r--r--. 1 root root unconfined_u:object_r/httpd_sys_content_t:0 3 cen 27 12:48 test.html
[rookie@andrievskaya html]$
```

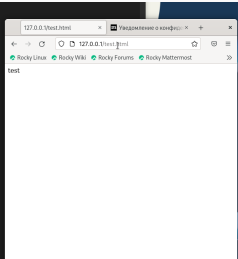
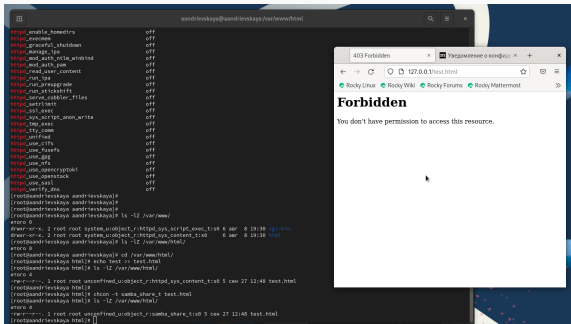


Figure 2: создание html-файла и доступ по http

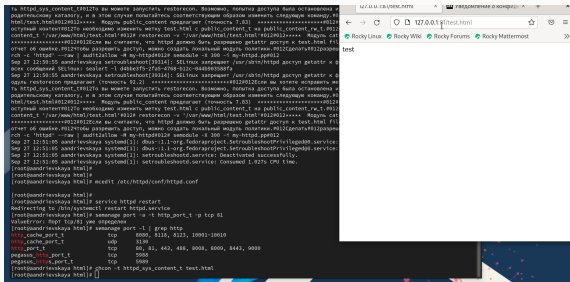


## Изменение контекста безопасности



### Figure 3: ошибка доступа после изменения контекста

## Переключение порта и восстановление контекста безопасности



### 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.