

# Знакомство с SELinux

---

Андрей Грыцькив НБИ-01-20

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

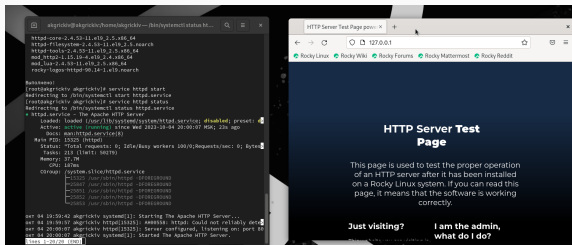
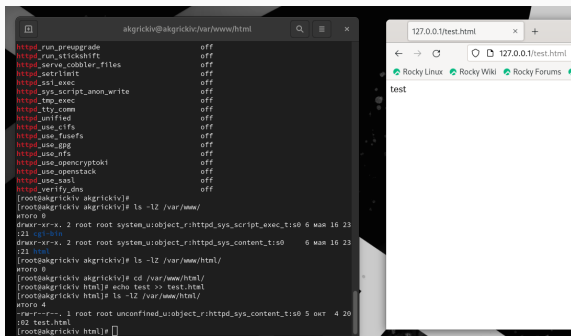


Figure 1: запуск http

# Создание HTML-файла



The screenshot shows a terminal window on the left and a web browser on the right. The terminal window is titled 'akgrickiv@akgrickiv:/var/www/html' and displays the following commands and output:

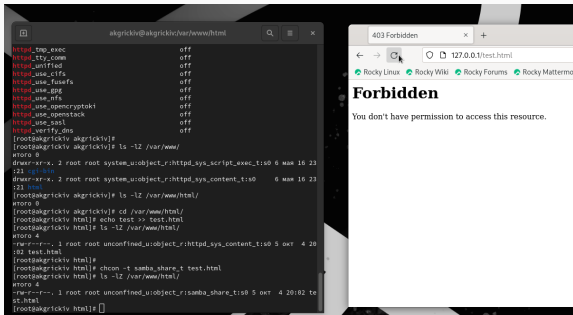
```
httpd_run_preupgrade      off
httpd_run_stickshift      off
httpd_serve_cobbler_files off
httpd_setrlimit           off
httpd_ssl_exec            off
httpd_sys_script_anon_write off
httpd_tmp_exec            off
httpd_tty_comm            off
httpd_unified             off
httpd_use_cifs            off
httpd_use_fusefs          off
httpd_use_gpg             off
httpd_use_nfs             off
httpd_use_openssl         off
httpd_use_openssl         off
httpd_use_openssl         off
httpd_use_openssl         off
httpd_verify_dns          off
[root@akgrickiv akgrickiv]#
[root@akgrickiv akgrickiv]# ls -lZ /var/www/
иторо 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мар 16 23
:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мар 16 23
:21 html
[root@akgrickiv akgrickiv]# ls -lZ /var/www/html/
иторо 0
[root@akgrickiv akgrickiv]# cd /var/www/html/
[root@akgrickiv html]# echo test >> test.html
[root@akgrickiv html]# ls -lZ /var/www/html/
иторо 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 окт 4 20
:02 test.html
[root@akgrickiv html]#
```

The web browser on the right shows the URL '127.0.0.1/test.html' and the content 'test'.

Figure 2: создание html-файла и доступ по http



## Изменение контекста безопасности



### Figure 3: ошибка доступа после изменения контекста



## **Выводы**

---

## Результаты выполнения лабораторной работы

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