

# Знакомство с SELinux

---

Иван Чернов

7 марта, 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

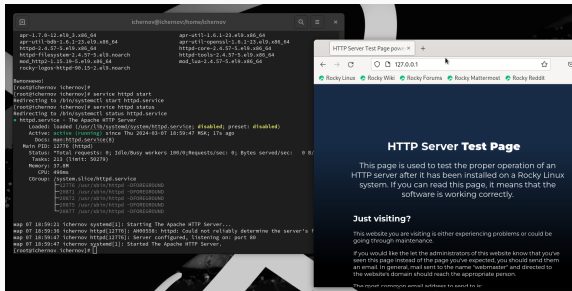
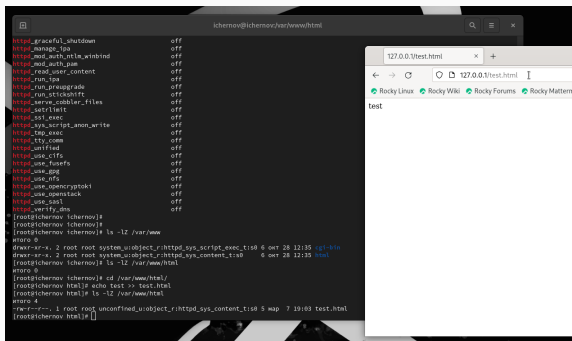


Figure 1: запуск http

# Создание HTML-файла



The image shows a terminal window on the left and a web browser on the right. The terminal window is titled 'ichernov@ichernov:~/var/www/html' and displays a list of SELinux booleans, all set to 'off'. Below this, the user runs 'ls -l /var/www' showing a directory 'html' with permissions 'drwxr-xr-x'. Then, the user runs 'cd /var/www/html/' and 'echo test >> test.html'. Finally, the user runs 'ls -l /var/www/html' showing the file 'test.html' with permissions 'drwxr-xr-x'. The web browser on the right is titled '127.0.0.1/test.html' and shows the content 'test'.

```
ichernov@ichernov:~/var/www/html
httpd_graceful_shutdown off
httpd_manage_ipo 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_sctkshim off
httpd_serve_cobbler_files off
httpd_satellite off
httpd_ssl_exec off
httpd_sys_script_anon_write off
httpd_tap_exec off
httpd_tty_core off
httpd_unified 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_deb off
[root@ichernov ~]#
[root@ichernov ~]#
[root@ichernov ~]# ls -l /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 oct 28 12:15 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 oct 28 12:15 html
[root@ichernov ~]# cd /var/www/html/
[root@ichernov ~]# echo test >> test.html
[root@ichernov ~]# ls -l /var/www/html
total 0
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 54p 7 19:03 test.html
[root@ichernov ~]#
```

Figure 2: создание html-файла и доступ по http



# Изменение контекста безопасности

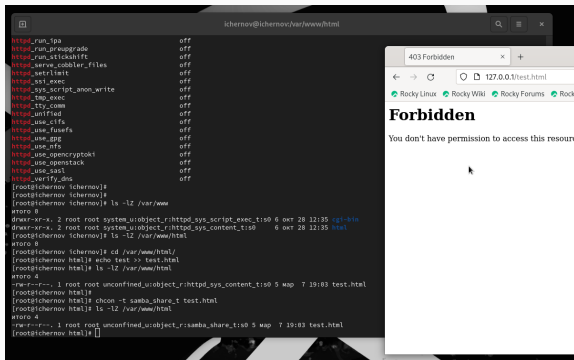


Figure 3: ошибка доступа после изменения контекста



## **Выводы**

---

# Результаты выполнения лабораторной работы

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