

Знакомство с SELinux

Алина Молокова

10 апреля, 2025, 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

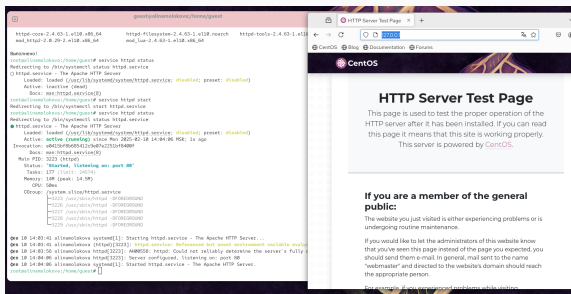
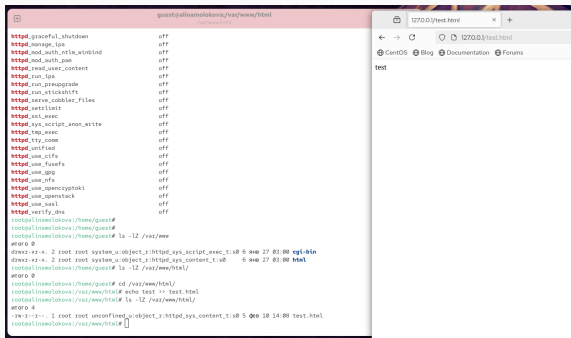


Рис. 1: запуск http

Создание HTML-файла



The screenshot displays a terminal window on the left and a web browser on the right. The terminal window shows the configuration of the httpd service, listing various modules and their status (all are 'off'). It then shows the user navigating to the /var/www/html directory and creating a test.html file using the 'echo' command. Finally, it shows the user running a command to start the httpd service. The web browser on the right shows the content of the test.html file, which is 'test'.

```
guest@galinamolokova:/var/www/html
$ cat /etc/httpd/conf/httpd.conf | grep -v ^# | grep -v ^$ | sort -u | xargs -n 1 -I {} sh -c 'echo {} | httpd -t'
httpd_graceful_shutdown off
httpd_manage_ipa off
httpd_mod_auth_mtls_winsbind 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_util_limit off
httpd_ssi_exec off
httpd_sys_script_anon_write off
httpd_ttp_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_ssl off
httpd_verify_dso off
root@galinamolokova:/home/guest#
root@galinamolokova:/home/guest# ls -lZ /var/www/html/
-rw-r--r-- 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 640 27 03:00 cgi-bin
-rw-r--r-- 2 root root system_u:object_r:httpd_sys_content_t:s0 640 27 03:00 html
root@galinamolokova:/home/guest# ls -lZ /var/www/html/
-rw-r--r-- 2 root root system_u:object_r:httpd_sys_content_t:s0 640 27 03:00 test.html
root@galinamolokova:/var/www/html# echo test > test.html
root@galinamolokova:/var/www/html# ls -lZ /var/www/html/
-rw-r--r-- 2 root root system_u:object_r:httpd_sys_content_t:s0 640 27 03:00 test.html
root@galinamolokova:/var/www/html#
```

127.0.0.1/test.html

test

Рис. 2: создание html-файла и доступ по http

Изменение контекста безопасности

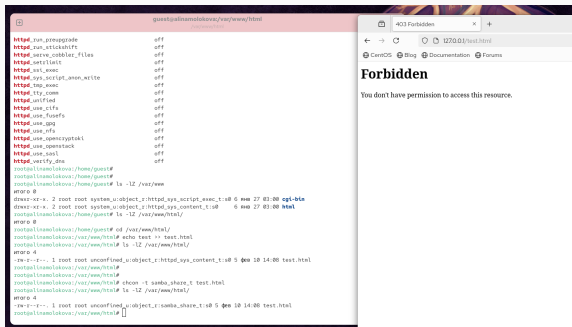


Рис. 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста безопасности

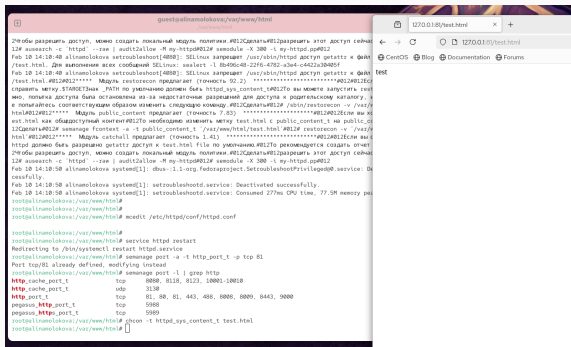


Рис. 4: доступ по http на 81 порт

Выводы

Результаты выполнения лабораторной работы

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