

Знакомство с SELinux

Мари Карапетян

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.

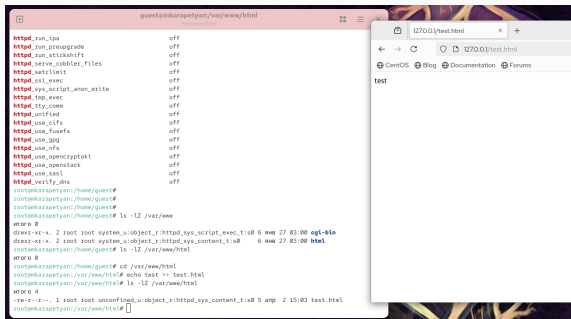
Apache – это свободное программное обеспечение для размещения веб-сервера. Он хорошо показывает себя в работе с масштабными проектами, поэтому заслуженно считается одним из самых популярных веб-серверов. Кроме того, Apache очень гибок в плане настройки, что даёт возможность реализовать все особенности 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

Создание HTML-файла



The screenshot shows a terminal window on the left and a web browser on the right. The terminal window is titled 'guest@mkarapetyan:/var/www/html' and displays a list of services that are turned off, followed by a series of commands to create and access an HTML file. The web browser on the right shows the file '127.0.0.1/test.html' with the content 'test'.

```
httpd_run_ipa off
httpd_run_pcreupgrade off
httpd_run_webkitohifs off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssl_exec off
httpd_sys_script_unon_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_sasl off
httpd_verify_dns off
root@mkarapetyan:/home/guest#
root@mkarapetyan:/home/guest#
root@mkarapetyan:/home/guest#
root@mkarapetyan:/home/guest# ls -lZ /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 Nov 27 03:00 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 Nov 27 03:00 html
root@mkarapetyan:/home/guest# ls -lZ /var/www/html
total 0
root@mkarapetyan:/home/guest# cd /var/www/html
root@mkarapetyan:/var/www/html# echo test >> test.html
root@mkarapetyan:/var/www/html# ls -lZ /var/www/html
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 Nov 27 15:03 test.html
root@mkarapetyan:/var/www/html#
```

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

Изменение контекста безопасности

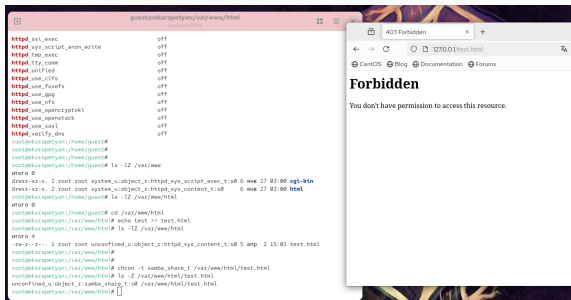


Рис. 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста безопасности

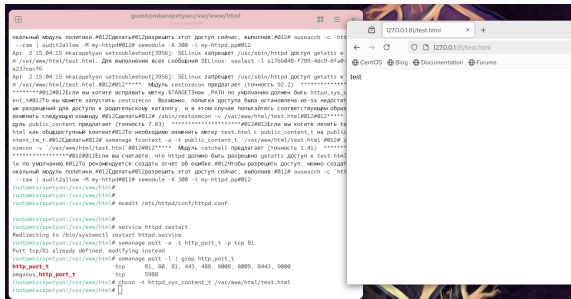


Рис. 4: доступ по http на 81 порт

Выводы

Результаты выполнения лабораторной работы

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