

Знакомство с SELinux

Власкин Никита Романович

18 июня, 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

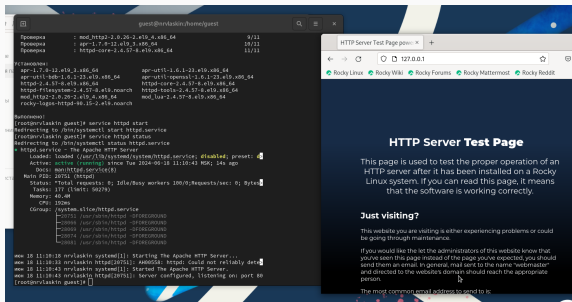
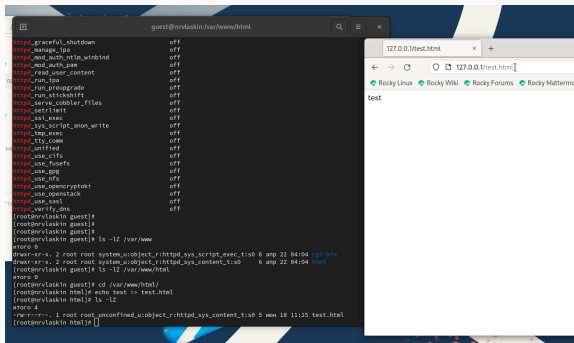


Figure 1: запуск http

Создание HTML-файла



The screenshot shows a terminal window with a list of configuration options for a web server, all set to 'off'. The user then navigates to the directory `/var/www/html` and creates a file named `test.html` containing the text `test`. Finally, the user opens a web browser at the address `127.0.0.1/test.html`, which displays the content of the file.

```
guest@nrvlaskin:/var/www/html
httpd_graceful_shutdown off
httpd_manage_ipa 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_sclchk 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_com 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_doc off
[root@nrvlaskin guest]#
[root@nrvlaskin guest]#
[root@nrvlaskin guest]# ls -l /var/www
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 amp 22 04:04 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 amp 22 04:04 html
[root@nrvlaskin guest]# ls -l /var/www/html
total 0
[root@nrvlaskin guest]# cd /var/www/html/
[root@nrvlaskin html]# echo test >> test.html
[root@nrvlaskin html]# ls -l
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 mon 18 11:15 test.html
[root@nrvlaskin html]#
```

127.0.0.1/test.html

test

Figure 2: создание html-файла и доступ по http

Изменение контекста безопасности

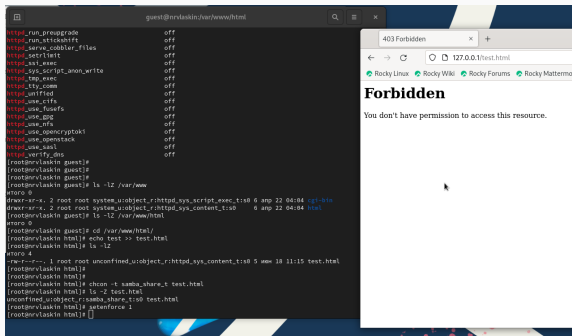


Figure 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста без-опасности

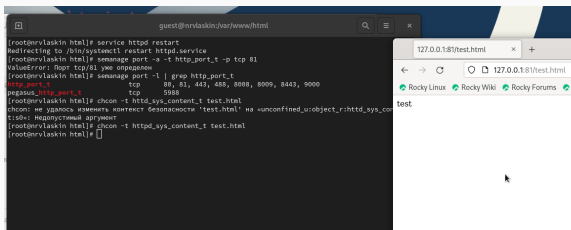


Figure 4: доступ по http на 81 порт

Выводы

Результаты выполнения лабораторной работы

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