

Знакомство с SELinux

Герра Гарсия Паола Валентина

9 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

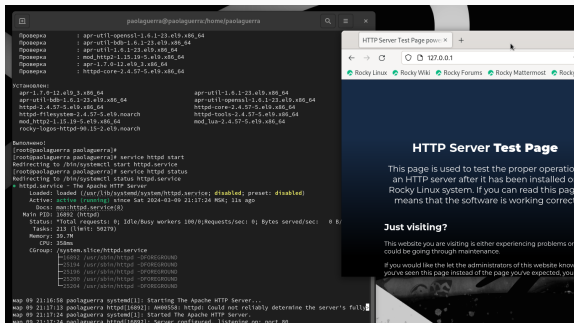
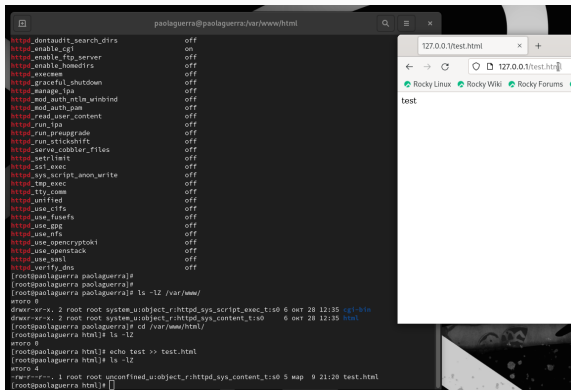


Figure 1: запуск http

Создание HTML-файла



The screenshot shows a terminal window on a Rocky Linux system. The terminal output lists various httpd configuration options, all set to 'off'. The user then navigates to the directory /var/www/html and creates a file named test.html with the content 'test'. Finally, the user opens a web browser at the address 127.0.0.1/test.html, which displays the word 'test'.

```
paolaguerra@paolaguerra: /var/www/html
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execuser off
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_sclistshift off
httpd_serve_cobbler_files off
httpd_setlimit off
httpd_ssl_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_sasl off
httpd_verify_dns off
[paolaguerra@paolaguerra ~]$ cd /var/www/html/
[paolaguerra@paolaguerra ~]$ ls -l /var/www/html/
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 окт 28 12:35 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 окт 28 12:35 html
[paolaguerra@paolaguerra ~]$ cd /var/www/html/
[paolaguerra@paolaguerra ~]$ ls -l
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 5 мар 9 21:20 test.html
[paolaguerra@paolaguerra ~]$
```

Figure 2: создание html-файла и доступ по http

Изменение контекста безопасности

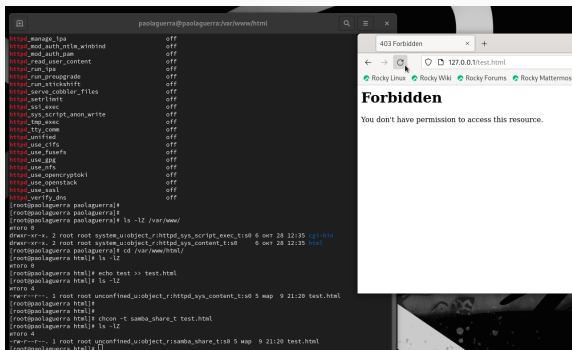


Figure 3: ошибка доступа после изменения контекста

Выводы

Результаты выполнения лабораторной работы

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