

Знакомство с SELinux

Алёна Лебедева

29 сентября, 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 НТТР-сервера

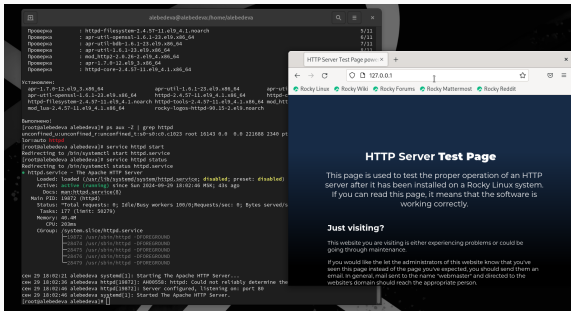
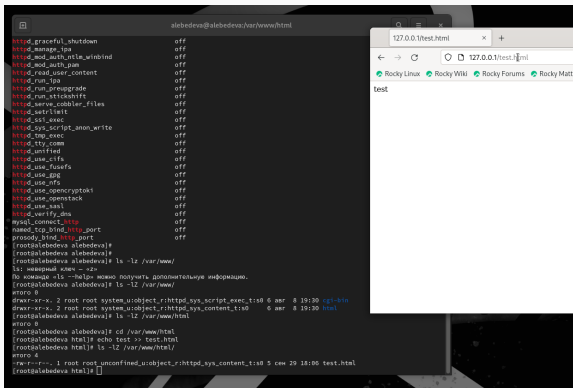


Figure 1: запуск http

Создание HTML-файла



The image shows a terminal window on the left and a web browser on the right. The terminal window is titled 'alebedeva@alebedeva:/var/www/html' and displays a list of services that are all 'off'. The user then runs 'ls -l /var/www/' and sees the directory contents. They then run 'echo test >> test.html' to create the file. Finally, they run 'ls -l /var/www/html/' and see the file 'test.html' with permissions '-rw-r--r--'. The web browser on the right shows the URL '127.0.0.1/test.html' and displays the word 'test'.

```
alebedeva@alebedeva:/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_ttksshift off
httpd_serve_cobbler_files off
httpd_setrlimit off
httpd_ssl_exec off
httpd_sys_script_anon_write off
httpd_tap_exec off
httpd_tty_com off
httpd_ufind off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_pg off
httpd_use_nfs off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_sasl off
httpd_verify_dns off
mysql_connect_http off
named_tcp_bind_http_port off
prosody_bind_http_port off
alebedeva@alebedeva:/var/www/html$
alebedeva@alebedeva:/var/www/html$ ls -l /var/www/
total 8
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 apr  8 19:30 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 apr  8 19:30 html
alebedeva@alebedeva:/var/www/html$
alebedeva@alebedeva:/var/www/html$ cd /var/www/html
alebedeva@alebedeva:/var/www/html$ echo test >> test.html
alebedeva@alebedeva:/var/www/html$ ls -l /var/www/html/
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 apr 29 18:06 test.html
alebedeva@alebedeva:/var/www/html$
```

Figure 2: создание html-файла и доступ по http

Изменение контекста безопасности

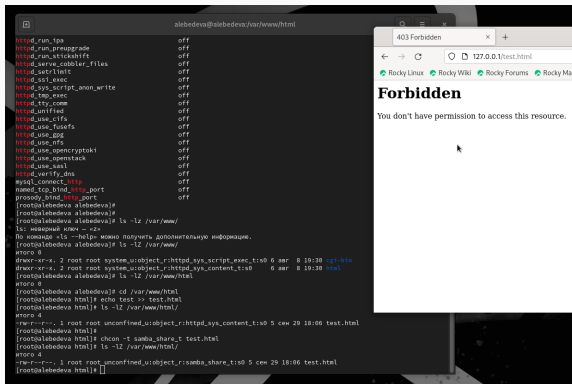


Figure 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста без-опасности

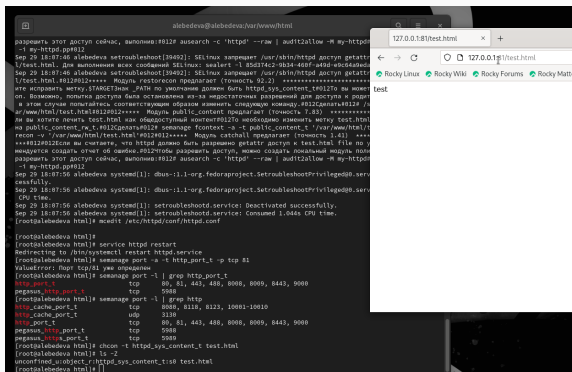


Figure 4: доступ по http на 81 порт

Выводы

Результаты выполнения лабораторной работы

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