

Знакомство с SELinux

Иовлев Максим

3 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

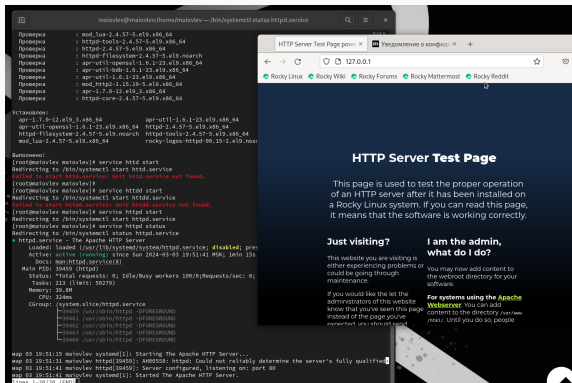
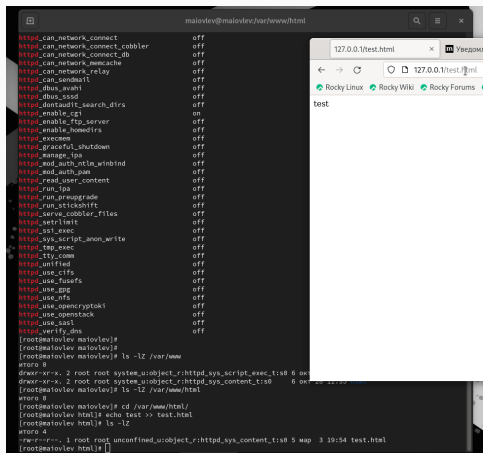


Figure 1: запуск http

Создание HTML-файла



The screenshot displays a terminal window with a dark background. The terminal shows the configuration of a web server, with various settings being turned on or off. The configuration includes settings for network connectivity, email, and various services. After the configuration, the user navigates to the directory `/var/www/html/` and creates a file named `test.html` containing the text `test`. The terminal output shows the following commands and their results:

```
httpd_can_network_connect off
httpd_can_network_connect_cobbler off
httpd_can_network_connect_db off
httpd_can_network_memcache off
httpd_can_network_relay off
httpd_can_sendmail off
httpd_dbus_avalahi off
httpd_dbus_tssd off
httpd_dontaudit_search_dirs off
httpd_enable_cgi on
httpd_enable_ftp_server off
httpd_enable_homedirs off
httpd_execadm off
httpd_graceful_shutdown off
httpd_manage_ipa off
httpd_mod_authn_tlm_winbind off
httpd_mod_auth_pam off
httpd_read_user_content off
httpd_run_ipa off
httpd_run_premupgrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setlimit off
httpd_ssl_exec off
httpd_sys_script_anon_write off
httpd_tap_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_dns off
[root@malovlev malovlev]#
[root@malovlev malovlev]#
[root@malovlev malovlev]# ls -lZ /var/www
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 on
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 on
[root@malovlev malovlev]# ls -lZ /var/www/html
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 on
[root@malovlev malovlev]# cd /var/www/html/
[root@malovlev html]# echo test >> test.html
[root@malovlev html]# ls -lZ
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 map 3 10:54 test.html
[root@malovlev html]#
```

Overlaid on the right side of the terminal is a web browser window. The address bar shows the URL `127.0.0.1/test.html`. The page content displays the word `test`, which is the content of the file created in the terminal.

Figure 2: создание html-файла и доступ по http

Изменение контекста безопасности

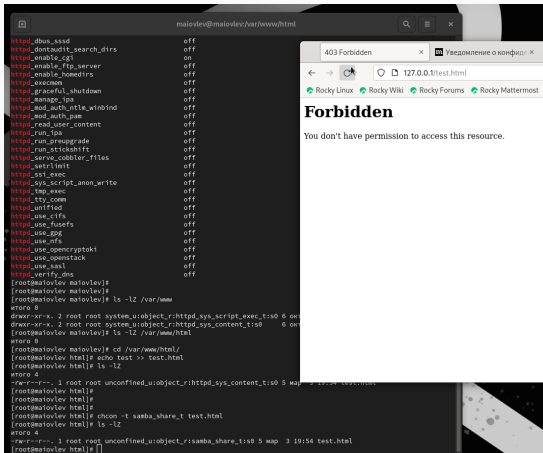


Figure 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста безопасности

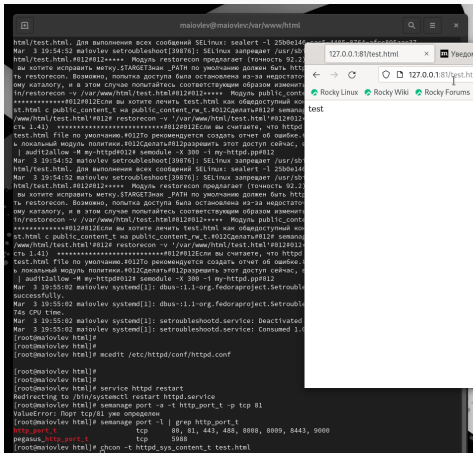


Figure 4: доступ по http на 81 порт

Выводы

Результаты выполнения лабораторной работы

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