

Знакомство с SELinux

Любимов Дмитрий Андреевич

9 октября, 2023, 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

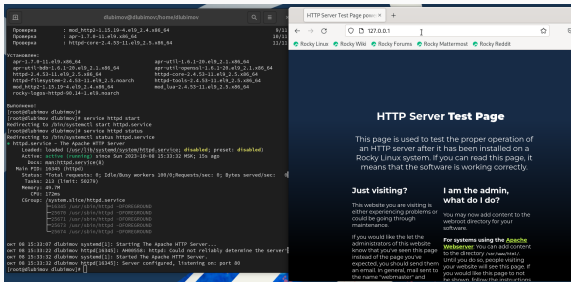
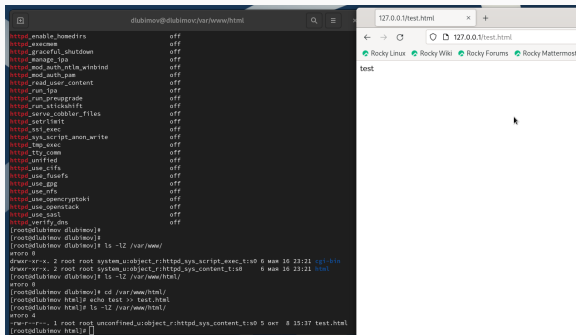


Figure 1: запуск http

Создание HTML-файла



The screenshot displays a terminal window on the left and a web browser on the right. The terminal shows the configuration of various httpd modules as 'off', followed by commands to create a directory, write a file, and serve it. The browser on the right shows the content of the file at the specified URL.

```
dlubimov@dlubimov:~/var/www/html$  
httpd_enable_bmodir      off  
httpd_enable_bmodir      off  
httpd_graceful_shutdown  off  
httpd_manage_ipa         off  
httpd_mod_auth_ntlm_bind  off  
httpd_mod_auth_pam       off  
httpd_read_user_content  off  
httpd_run_ipa            off  
httpd_run_preupgrade     off  
httpd_run_stickshift     off  
httpd_serve_cobbler_files off  
httpd_setlimit           off  
httpd_ssl_exec           off  
httpd_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_mfs            off  
httpd_use_openssl        off  
httpd_use_openssl        off  
httpd_use_sasl           off  
httpd_verify_dns         off  
[root@dlubimov dlubimov]#  
[root@dlubimov dlubimov]# ls -lZ /var/www/  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 16 23:21 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 16 23:21 html  
[root@dlubimov dlubimov]# ls -lZ /var/www/html/  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 16 23:21 test.html  
[root@dlubimov dlubimov]# cd /var/www/html/  
[root@dlubimov html]# echo test >> test.html  
[root@dlubimov html]# ls -lZ /var/www/html/  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 окт 8 15:37 test.html  
[root@dlubimov html]#
```

The browser window shows the URL `127.0.0.1/test.html` and the content `test`.

Figure 2: создание html-файла и доступ по http

Изменение контекста безопасности

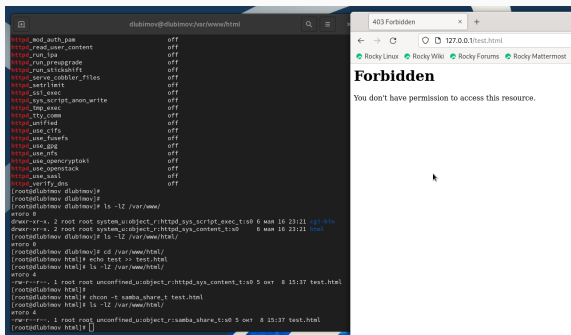


Figure 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста безопасности

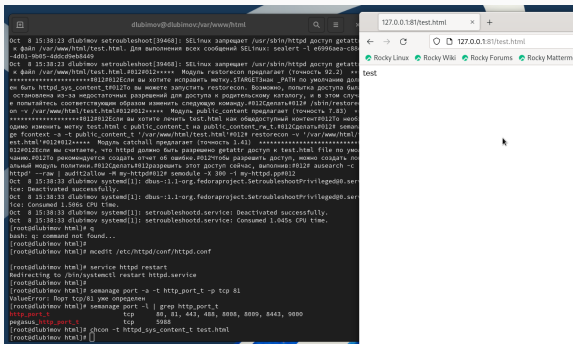


Figure 4: доступ по http на 81 порт

Выводы

Результаты выполнения лабораторной работы

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