

Знакомство с SELinux

Еде Мак Дональд Чуквума

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 HTTP-сервера

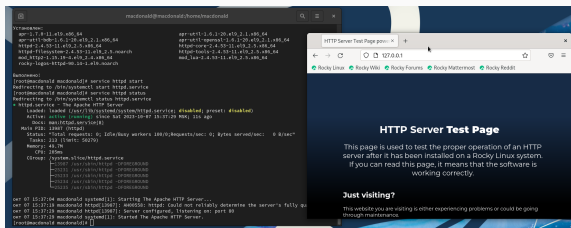
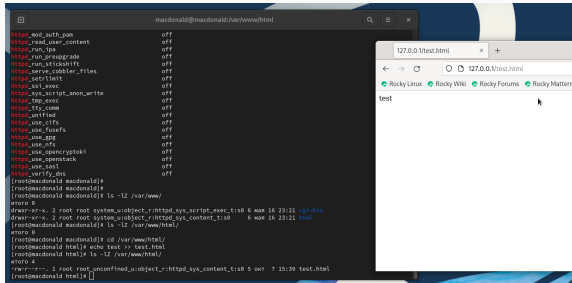


Figure 1: запуск http

Создание HTML-файла



```
macdonald@macdonald: /var/www/html
httpd_mod_auth_pam off
httpd_mod_auth_unix_user_content off
httpd_run_ipa off
httpd_run_groovegrade off
httpd_run_stickshift off
httpd_serve_cobbler_files off
httpd_setlimit off
httpd_ssl_exec off
httpd_sys_script_anon_write off
httpd_tag_exec off
httpd_tty_comm off
httpd_unified off
httpd_use_cifs off
httpd_use_fusefs off
httpd_use_egg off
httpd_use_efs off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_use_openssl off
httpd_verify_dns off
[macdonald@macdonald ~]$
[macdonald@macdonald ~]$ ls -l /var/www/
total 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:sb 6 мая 16 23:21 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:sb 6 мая 16 23:21 html
[macdonald@macdonald ~]$ ls -l /var/www/html/
total 0
[macdonald@macdonald ~]$ cd /var/www/html/
[macdonald@macdonald ~]$ echo test >> test.html
[macdonald@macdonald ~]$ ls -l /var/www/html/
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:sb 5 окт 7 15:39 test.html
[macdonald@macdonald ~]$
```

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

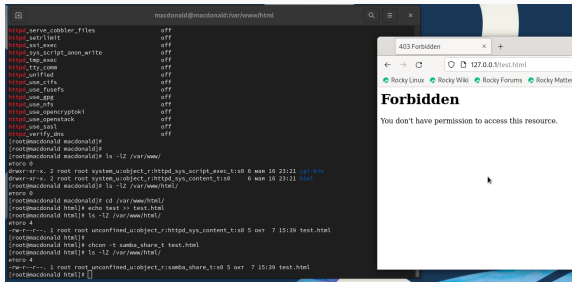


Figure 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста безопасности

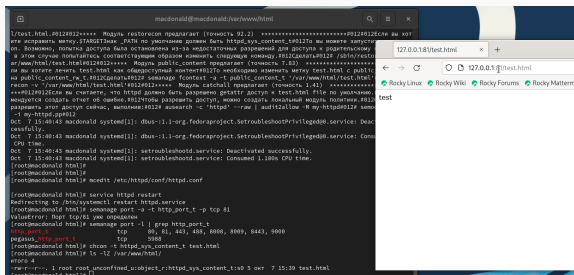


Figure 4: доступ по http на 81 порт

Выводы

Результаты выполнения лабораторной работы

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