Знакомство с SELinux

Арутюнян Эрик 3 октября, 2024, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Теоретическое введение

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.

Теоретическое введение

Арасhe – 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, Арасhe 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 SELinx на практике совместно с веб-сервером Apache

Выполнение лабораторной работы

Запуск НТТР-сервера



Рис. 1: запуск http

Создание HTML-файла

```
## E (X)
                                                                                                                 270.03/test.html
httpd_setrlinit
                                                                                                             ← → C O D 127003/test.html
httpd_sys_script_anon_write
                                                                                                            ⊕ CentOS ⊕ Blog ⊕ Documentation ⊕ Forums
httpd_tmp_exec
httpd tty comm
httpd unified
                                          011
httpd_use_cifs
httpd_use_fusefs
httpd_use_cpq
httpd_use_nfs
httpd_use_openstack
httpd_use_sasl
httpd verify dos
 rootjesrutynyan:/home/guest# ls -lZ /var/www
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ### 27 03:00 ogi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 mms 27 03:00 html
 contreasutymyan:/war/www/html# echo test >> test.html
-rw-r--r-. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 Map 30 14:45 test.html
rootsearutynyan:/war/wan/html#
```

Рис. 2: создание html-файла и доступ по http

Изменение контекста безопасности



Рис. 3: ошибка доступа после изменения контекста

Переключение порта и восстановление контекста безопасности



Рис. 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.