Знакомство с SELinux

Гуламова Е.М.

10 апреля, 2025, 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

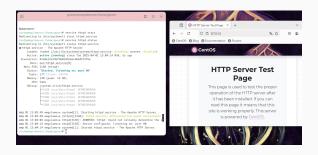


Рис. 1: запуск http

Создание HTML-файла

```
httpd_setrlinit
                                                                                                 TZ70.0.Utest.html
 ttpd_ssi_exec
httpd_sys_script_anon_write
                                                                                                → C O D 1270,01/test.html
 ttpd two exec
nttpd_tty_comm
                                                                                             ⊕ CentOS ⊕ Blog ⊕ Documentation ⊕ Forums
httpd_unified
ttpd_use_cifs
 ttpd_use_fusefs
ttpd use opo
ttpd use ofs
 ttpd_use_opencryptoki
httpd_use_openstack
httpd_use_sasl
httpd verify dea
 ootmengulamova:/home/guest#
 ootgengulamova:/home/guest# ls -lZ /var/www
frwxr-xr-x. 2 root root system u:object r:httpd sys script exec t:s0 6 swa 27 03:00 coi-bim
draxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 mem 27 03:00 html
 ootmengulamova:/home/guest# ls -lZ /var/www/html
 ootmengulamova:/home/guest# cd /var/www/html
rootsengulamova:/var/www/html# echo test >> test.html
 rw-r--r-. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 5 amp 1 15:06 test.ht
```

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.