Знакомство с SELinux

Джало Дмитрий 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

```
root@ddzhalo:/home/guest# ps aux -Z | grep httpd
system_u:system_r:httpd_t:s0 root
                                        3253 0.0 0.2 18544 10748 ?
                                                                          Ss 15:52 0:00 /usr/
sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0
                                        3258 0.0 0.1 18200 5048 ?
                                                                               15:53 0:00 /usr/
                             apache
sbin/httpd -DFOREGROUND
system u:system r:httpd t:s0
                             apache
                                        3259 0.0 0.2 2353808 8308 ?
                                                                               15:53 0:00 /usr/
sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0
                                        3260 0.0 0.2 2157136 8212 ?
                                                                               15:53 0:00 /usr/
                             apache
sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache
                                        3267 0.0 0.1 2222672 7232 ?
                                                                          Sl 15:53 0:00 /usr/
sbin/httpd -DFOREGROUND
unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023 root 3870 0.0 0.0 227712 2312 pts/0 S+ 15:54 0:
00 grep --color=auto httpd
root@ddzhalo:/home/quest#
```

Рис. 1: запуск http

Создание HTML-файла

```
httpd serve cobbler files
httpd.setrlinit
                                                                                                    ← → C O D 1270.03/test.html ☆ ⊕ ⊕ ሷ =
httpd_ssi_exec
httpd_sys_script_enon_write
                                                                                                   ⊕ CentOS ⊕ Blog ⊕ Documentation ⊕ Forums
httpd top exec
httpd tty com
httpd_unified
httpd_use_cifs
httpd use fusefs
httpd_use_opg
httpd_use_nfs
httpd_use_opencryptoki
httpd_use_openstack
httpd use seal
httpd_verify_das
 rooteddrhelo:/home/quest# ls -lZ /war/maw
 drexr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 sem 27 03:00 cgi-bin
 drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 mem 27 03:00 btml
  octodznalo:/home/guest# od /var/www/html
 -rw-r--r-. 1 root root uncomfined_u:object_r:httpd_sys_content_t:s0 5 amp 1 15:96 test.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

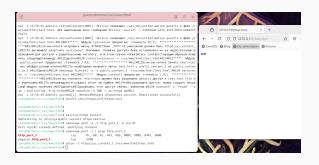


Рис. 4: доступ по http на 81 порт

Выводы

Результаты выполнения лабораторной работы

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