Знакомство с SELinux

Баазова Нина

2 мая, 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

```
□ 1270.03/test.html
httpd run preupgrade
httpd.run.stickshift
                                                                                                           ← → C O D 97003/test.html
httpd_serve_cobbler_files
httpd_setrlinit
                                                                                                          ⊕ CentOS ⊕ Blog ⊕ Documentation ⊕ Forums
httpd_sst_exec
httpd_sys_script_anon_write
httpd two exec
httpd_tty_conn
httpd unified
httpd use cifs
httpd_use_fusefs
httpd_use_gpq
httpd_use_nfs
httpd_use_opencryptoki
httpd use sast
httpd verify dos
mysgl connect http
named top bind http port
prosedy_bind_http_port
 cot@minabaszova:/home/minabaszova# ls -12 /var/www
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 mms 27 03:00 ogi-bin
drace-xr-x, 2 root root system u object r:httpd sys content t:s0 6 mem 27 03:00 html
 coteninabaszova:/home/ninabaszova# ls -lZ /var/enw/html
 ootgeninabaazova:/var/www/html# echo test >> test.html
 ootgeinabaarova:/var/www/html# ls -lZ /var/www/html
 rw-r--r-. 1 root root unconfingd_u:object_r:httpd_sys_content_t:s0 5 dem 11 12:24 test.html
```

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

Изменение контекста безопасности

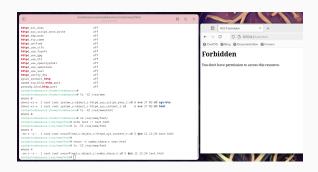


Рис. 3: ошибка доступа после изменения контекста

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.