Знакомство с SELinux

Алькамаль Ибрахим Мохсейн Мохаммед Али 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_ssi_exec
httpd_sys_script_anon_write
                                                                                                         127.0.0.1/test.html
httpd_tmp_exec
httpd_tty_conn
                                                                                                     ← → C ○ □ 1270.0.1/test.html ☆
httpd unified
                                         off
httpd_use_cifs
                                                                                                     ⊕ CentOS ⊕ Blog ⊕ Documentation ⊕ Forums
httpd use fusefs
httpd_use_gpg
httpd_use_nfs
httpd_use_opencryptoki
httpd_use_openstack
httpd_use_sasl
httpd_verify_dns
root@Ebrahim:/home/guest# ls -lZ /war/www
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 mem 27 03:00 cgi-bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 mmm 27 83:00 html
root@Ebrahim:/home/guest# cd /var/www/html
 rootsEbrahim:/var/www/html# echo test >> test.html
 rootgEbrahim:/var/www/html# ls -12 /var/www/html
 rw-r--r-. 1 root root unconfined_u:object_r:httpd_sys_content_t:s8 5 amp 4 18:04 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.