Знакомство с SELinux

Краснова Диана Владимировна

14 октября, 2023, Москва, Россия

1 Цели и задачи

1.1 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.

1.2 Теоретическое введение

Apache – 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, Apache очень гибок в плане настройки, что даёт возможность реализовать все особенности размещаемого веб-ресурса.

1.3 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

2 Выполнение лабораторной работы

2.1 Запуск HTTP-сервера

```
[guest@dvkrasnova ~]$ touch simpleid.c
[guest@dvkrasnova ~]$ open simpleid.c
Couldn't get a file descriptor referring to the console
[guest@dvkrasnova ~]$ cat simpleid.c
[guest@dvkrasnova ~]$ vim simpleid.c
[guest@dvkrasnova ~]$ cat simpleid.c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
int
main ()
{
uid_t uid = geteuid ();
gid_t gid = getegid ();
printf ("uid=%d, gid=%d\n", uid, gid);
return 0;
}
[guest@dvkrasnova ~]$ gcc simpleid.c -o simpleid
[guest@dvkrasnova ~]$
```

запуск http

2.2 Создание HTML-файла

```
[guest@dvkrasnova ~]$ id
uid=1002(guest) gid=1002(guest) groups=1002(guest) context=unconfined_u:unconfin
ed_r:unconfined_t:s0-s0:c0.c1023
[guest@dvkrasnova ~]$ ./simpleid
uid=1002, gid=1002
[guest@dvkrasnova ~]$
```

создание html-файла и доступ по http

2.3 Изменение контекста безопасности

```
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
int
main ()
{
uid_t real_uid = getuid ();
uid_t e_uid = geteuid ();
gid_t real_gid = getgid ();
gid_t e_gid = getegid () ;
printf ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
printf ("real_uid=%d, real_gid=%d\n", real_uid,
real_gid);
return 0;
}
```

ошибка доступа после изменения контекста

2.4 Переключение порта и восстановление контекста безопасности

```
[guest@dvkrasnova ~]$ su
Password:
[root@dvkrasnova guest]# chown root:guest /home/guest/simpleid2
[root@dvkrasnova guest]# chmod u+s /home/guest/simpleid2
[root@dvkrasnova guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 18312 Oct  6 14:30 simpleid2
[root@dvkrasnova guest]#
```

доступ по http на 81 порт

3 Выводы

3.1 Результаты выполнения лабораторной работы

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