Лабораторная №5

Основы информационной безопасности

Банникова Екатерина Алексеевна

Российский университет дружбы народов, Москва, Россия

НПМбд-01-19

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Цель лабораторной работы

- Изучить особенности работы с дополнительными атрибутами SetUID, SetGID и Sticky
- Изучить механизмы изменения индефикатора.

Задачи лабораторной работы

1. Создать программу, выводящую uid и gid, и посмотреть на вывод после добавления SetUID и SetGID битов.
2. Создать программу для чтения файлов и проверить вывод после добавления SetUID бита.
3. На примере папки /tmp изучить влияние Sticky бита на запись и удаление файлов.

Выполнение

Создаём файл simpleid2.c, который будет выводить uid и gid. При отсутствии дополнительных битов, она выводит информацию, совпадающую с выводом команды id.

```
[guest1@eabannikova ~]$ gcc simpleid2.c -o simpleid2
[guest1@eabannikova ~]$ ./simpleid2
e_uid=1002, e_gid=1002
real_uid=1002, real_gid=1002
[guest1@eabannikova ~]$
```

Figure 1: Результат работы simpleid2

Выполнение

С помощью команды chown меняем владельца файла на root и устанавливаем SetUID командой chmod u+s.

```
[eabannikova@eabannikova ~]$ sudo chown root:guest1 /home/guest1/simpleid2
[sudo] пароль для eabannikova:
[eabannikova@eabannikova ~]$ sudo chmod u+s /home/guest1/simpleid2
[eabannikova@eabannikova ~]$ ls -l /home/guest1/simpleid2
ls: невозможно получить доступ к '/home/guest1/simpleid2': Отказано в доступе
[eabannikova@eabannikova ~]$ sudo ls -l /home/guest1/simpleid2
-rwsrwxr-x. 1 root guest1 11336 окт  6 15:43 /home/guest1/simpleid2
[eabannikova@eabannikova ~]$
```

Figure 2: Установка SetUID-бита

Выполнение

После запуска видим, что uid сменилось на 0 (для root), в то время как в команде id uid всё ещё остался 1001

Figure 3: Результат работы simpleid2

Выполнение

С помощью команды chown меняем группу для файла и устанавливаем SetGID командой chmod g+s. Видим, что при запуске программы изменился вывод gid.

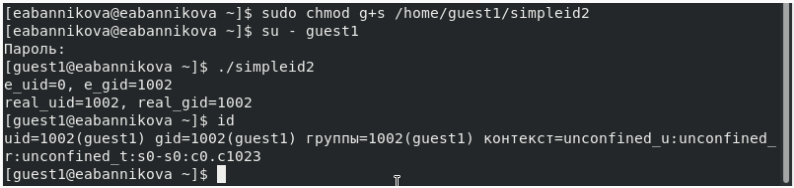

Figure 4: Установка SetGID-бита

Выполнение

Проводим над файлом file01.txt следующие действия: читаем его, дозаписываем и перезаписываем информацию, переименовываем. Эти действия проходят без ошибок. При попытке удаления возникает ошибка.

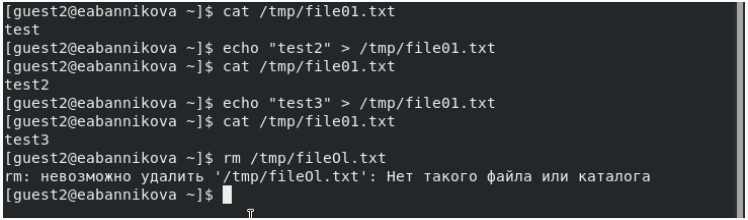

Figure 5: Наличие Sticky-бита

От имени суперпользователя удаляем sticku-бит командой chmod -t.

```
[eabannikova@eabannikova ~]$ su -
Пароль:
[root@eabannikova ~]# chmod -t /tmp
[root@eabannikova ~]# exit
выход
[eabannikova@eabannikova ~]$
```

Figure 6: Удаление Sticky-бита

Выполнение

Повторяем описанные ранее действия над файлом file01.txt. Теперь пользователь может удалить не принадлежащий ему файл.

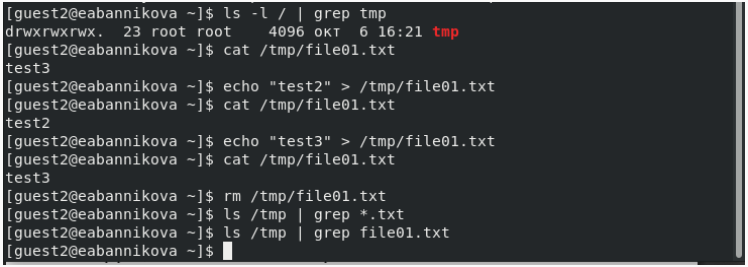

Figure 7: Отсутсвие Sticky-бита

Выводы

- Я изучила механизмы изменения идентификаторов.
- Получила практические навыки по работе с дополнительными атрибутами.