

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

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

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.

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`

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

После запуска видим, что uid сменилось на 0 (для root), в то время как в команде id uid всё ещё остался 1002

```
[guest1@eabannikova ~]$ ./simpleid2
e_uid=0, e_gid=1002
real_uid=1002, real_gid=1002
[guest1@eabannikova ~]$ id
uid=1002(guest1) gid=1002(guest1) группы=1002(guest1) контекст=unconfined_u:unconfined_
r:unconfined_t:s0-s0:c0.c1023
[guest1@eabannikova ~]$
```

Figure 3: Результат работы simpleid2

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

```
[eabannikova@eabannikova ~]$ sudo chmod g+s /home/guest1/simpleid2
[eabannikova@eabannikova ~]$ su - guest1
Пароль:
[guest1@eabannikova ~]$ ./simpleid2
e_uid=0, e_gid=1002
real_uid=1002, real_gid=1002
[guest1@eabannikova ~]$ id
uid=1002(guest1) gid=1002(guest1) группы=1002(guest1) контекст=unconfined_u:unconfined_
r:unconfined_t:s0-s0:c0.c1023
[guest1@eabannikova ~]$
```

Figure 4: Установка SetGID-бита

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

```
[guest2@eabannikova ~]$ cat /tmp/file01.txt
test
[guest2@eabannikova ~]$ echo "test2" > /tmp/file01.txt
[guest2@eabannikova ~]$ cat /tmp/file01.txt
test2
[guest2@eabannikova ~]$ echo "test3" > /tmp/file01.txt
[guest2@eabannikova ~]$ cat /tmp/file01.txt
test3
[guest2@eabannikova ~]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Нет такого файла или каталога
[guest2@eabannikova ~]$
```

Figure 5: Наличие Sticky-бита

От имени суперпользователя удаляем sticky-бит командой `chmod -t`.

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

Figure 6: Удаление Sticky-бита

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

```
[guest2@eabannikova ~]$ ls -l / | grep tmp
drwxrwxrwx. 23 root root 4096 окт 6 16:21 tmp
[guest2@eabannikova ~]$ cat /tmp/file01.txt
test3
[guest2@eabannikova ~]$ echo "test2" > /tmp/file01.txt
[guest2@eabannikova ~]$ cat /tmp/file01.txt
test2
[guest2@eabannikova ~]$ echo "test3" > /tmp/file01.txt
[guest2@eabannikova ~]$ cat /tmp/file01.txt
test3
[guest2@eabannikova ~]$ rm /tmp/file01.txt
[guest2@eabannikova ~]$ ls /tmp | grep *.txt
[guest2@eabannikova ~]$ ls /tmp | grep file01.txt
[guest2@eabannikova ~]$
```

Figure 7: Отсутствие Sticky-бита

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