

Лабораторная работа №5

Основы информационной безопасности

Балакирева Дарья Сергеевна

5 октября 2022

Российский университет дружбы народов, Москва, Россия

НПМбд-01-196

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

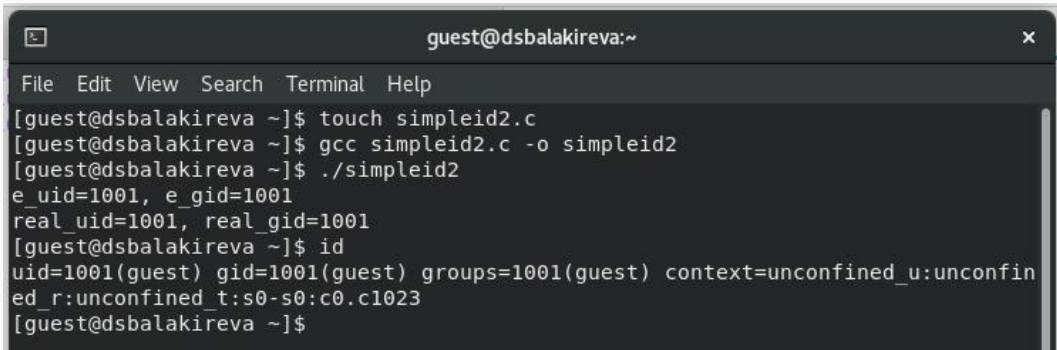
- Изучить особенности работы с дополнительными атрибутами SetUID, SetGID и Sticky.
- Изучить механизмы изменения идентификаторов.

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

Ход лабораторной работы

Создание файла

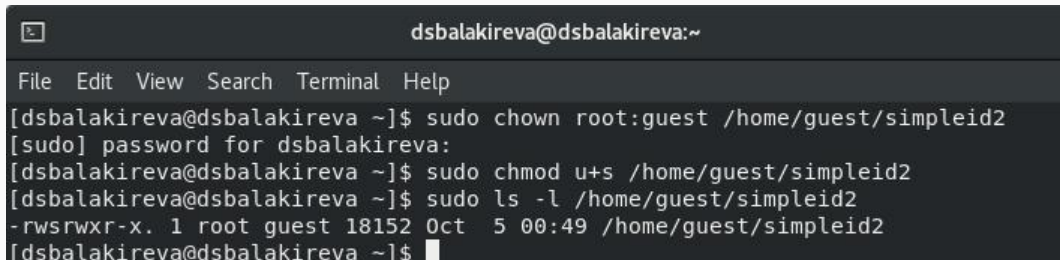
Создаём файл `simpleid2.c`, который будет выводить `uid` и `gid`. При отсутствии дополнительных битов, она выводит информацию, совпадающую с выводом команды `id`.

A terminal window titled 'guest@dsbalakireva:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
[guest@dsbalakireva ~]$ touch simpleid2.c
[guest@dsbalakireva ~]$ gcc simpleid2.c -o simpleid2
[guest@dsbalakireva ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@dsbalakireva ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@dsbalakireva ~]$
```

Figure 1: Результат работы `simpleid2`

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

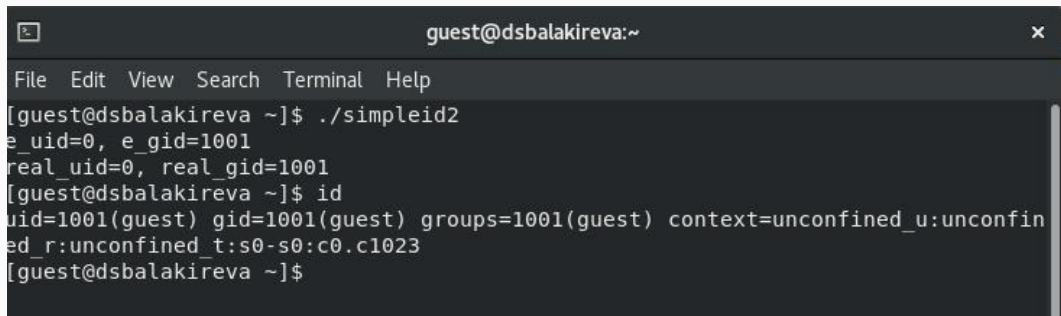


```
dsbalakireva@dsbalakireva:~  
File Edit View Search Terminal Help  
[dsbalakireva@dsbalakireva ~]$ sudo chown root:guest /home/guest/simpleid2  
[sudo] password for dsbalakireva:  
[dsbalakireva@dsbalakireva ~]$ sudo chmod u+s /home/guest/simpleid2  
[dsbalakireva@dsbalakireva ~]$ sudo ls -l /home/guest/simpleid2  
-rwsrwxr-x. 1 root guest 18152 Oct  5 00:49 /home/guest/simpleid2  
[dsbalakireva@dsbalakireva ~]$
```

Figure 2: Установка SetUID-бита

Запуск simpleid2

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

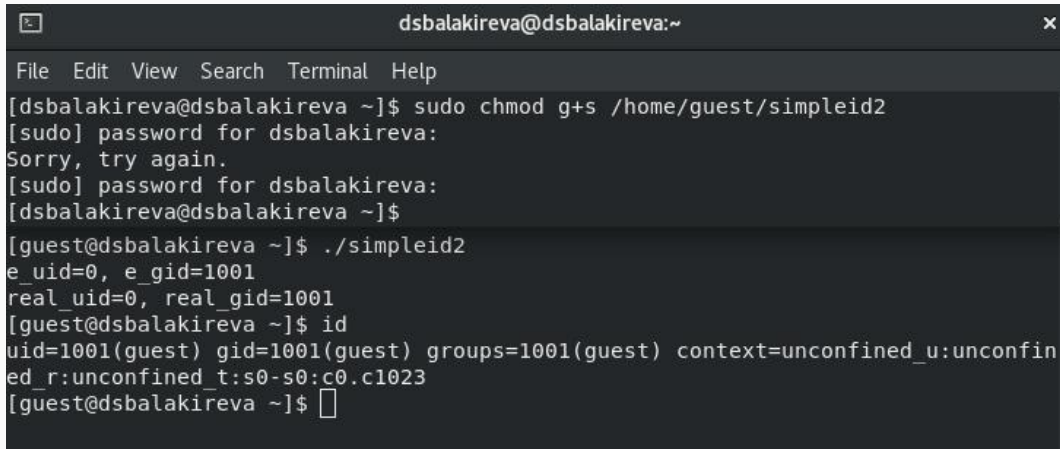


```
guest@dsbalakireva:~  
File Edit View Search Terminal Help  
[guest@dsbalakireva ~]$ ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=0, real_gid=1001  
[guest@dsbalakireva ~]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@dsbalakireva ~]$
```

Figure 3: Результат работы simpleid2

Установка SetGID-бита

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



```
dsbalakireva@dsbalakireva:~  
File Edit View Search Terminal Help  
[dsbalakireva@dsbalakireva ~]$ sudo chmod g+s /home/guest/simpleid2  
[sudo] password for dsbalakireva:  
Sorry, try again.  
[sudo] password for dsbalakireva:  
[dsbalakireva@dsbalakireva ~]$  
[guest@dsbalakireva ~]$ ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=0, real_gid=1001  
[guest@dsbalakireva ~]$ id  
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@dsbalakireva ~]$
```

Figure 4: Установка setGID-бита

Наличие Sticky-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.

```
[guest@dsbalakireva ~]$ su - guest2
Password:
[guest2@dsbalakireva ~]$ cat /tmp/file01.txt
test
[guest2@dsbalakireva ~]$ echo "test2" >> /tmp/file01.txt
[guest2@dsbalakireva ~]$ cat /tmp/file01.txt
test
test2
[guest2@dsbalakireva ~]$ echo "test3" > /tmp/file01.txt
[guest2@dsbalakireva ~]$ cat /tmp/file01.txt
test3
[guest2@dsbalakireva ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
```

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

```
[dsbalakireva@dsbalakireva ~]$ su -  
Password:  
[root@dsbalakireva ~]# chmod -t /tmp  
[root@dsbalakireva ~]# exit  
logout  
[dsbalakireva@dsbalakireva ~]$
```

Figure 6: Удаление Sticky-бита

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

```
[guest2@dsbalakireva ~]$ ls -l / | grep tmp
drwxrwxrwx. 16 root root 4096 Oct  5 01:33 tmp
[guest2@dsbalakireva ~]$ cat /tmp/file01.txt
test3
[guest2@dsbalakireva ~]$ echo "test2" >> /tmp/file01.txt
[guest2@dsbalakireva ~]$ cat /tmp/file01.txt
test3
test2
[guest2@dsbalakireva ~]$ echo "test3" > /tmp/file01.txt
[guest2@dsbalakireva ~]$ cat /tmp/file01.txt
test3
[guest2@dsbalakireva ~]$ rm /tmp/file01.txt
[guest2@dsbalakireva ~]$ ls /tmp | grep *txt
```

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