

# Лабораторная работа №5

## Основы информационной безопасности

---

Полиенко Анастасия Николаевна

23 сентября 2022

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 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

---

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

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

Figure 1: Результат работы `simpleid2`

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

```
[anpolienko@anpolienko ~]$ sudo chown root:guest /home/guest/simpleid2
[sudo] password for anpolienko:
[anpolienko@anpolienko ~]$ sudo chmod u+s /home/guest/simpleid2
[anpolienko@anpolienko ~]$ ls -l /home/guest/simpleid2
ls: cannot access '/home/guest/simpleid2': Permission denied
[anpolienko@anpolienko ~]$ sudo ls -l /home/guest/simpleid2
-rwsrwxr-x. 1 root guest 18152 Sep 21 01:09 /home/guest/simpleid2
```

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 1001.

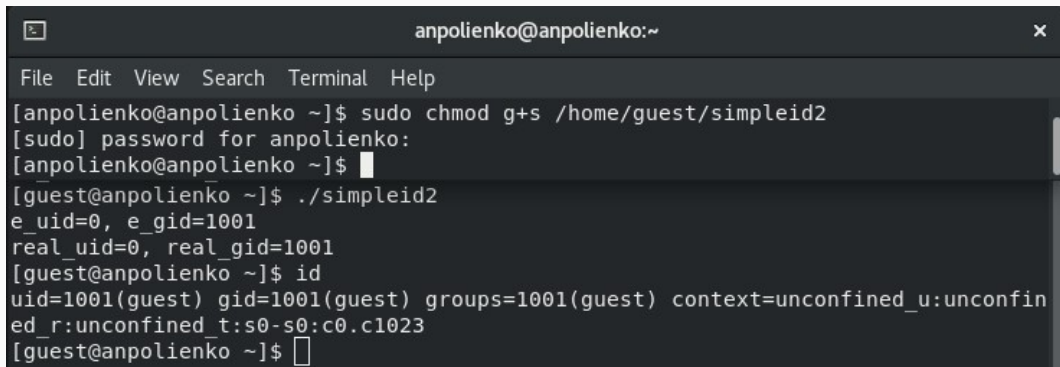
```
[guest@anpolienko ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=1001
[guest@anpolienko ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@anpolienko ~]$
```

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`.

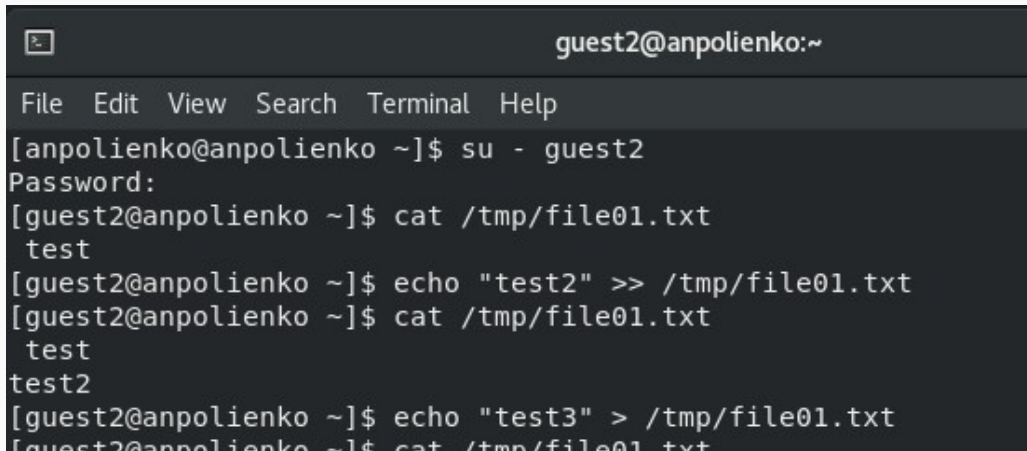


```
anpolienko@anpolienko:~  
File Edit View Search Terminal Help  
[anpolienko@anpolienko ~]$ sudo chmod g+s /home/guest/simpleid2  
[sudo] password for anpolienko:  
[anpolienko@anpolienko ~]$  
[guest@anpolienko ~]$ ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=0, real_gid=1001  
[guest@anpolienko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

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.



```
guest2@anpolienko:~  
File Edit View Search Terminal Help  
[anpolienko@anpolienko ~]$ su - guest2  
Password:  
[guest2@anpolienko ~]$ cat /tmp/file01.txt  
test  
[guest2@anpolienko ~]$ echo "test2" >> /tmp/file01.txt  
[guest2@anpolienko ~]$ cat /tmp/file01.txt  
test  
test2  
[guest2@anpolienko ~]$ echo "test3" > /tmp/file01.txt  
[guest2@anpolienko ~]$ cat /tmp/file01.txt
```

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

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

Figure 6: Удаление Sticky-бита

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

```
[guest2@anpolienko ~]$ ls -l / | grep tmp
drwxrwxrwx.  18 root root 4096 Sep 22 00:41 tmp
[guest2@anpolienko ~]$ cat /tmp/file01.txt
test3
[guest2@anpolienko ~]$ echo "test2" >> /tmp/file01.txt
[guest2@anpolienko ~]$ cat /tmp/file01.txt
test3
test2
[guest2@anpolienko ~]$ echo "test3" > /tmp/file01.txt
[guest2@anpolienko ~]$ cat /tmp/file01.txt
test3
[guest2@anpolienko ~]$ rm /tmp/file01.txt
[guest2@anpolienko ~]$ ls /tmp | grep *.txt
[guest2@anpolienko ~]$ ls /tmp | grep file01.txt
```

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