

# Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

---

Гаглов Олег Мелорович

7 октября, 2023, Москва, Россия

Российский Университет Дружбы Народов

# Цели и задачи

---

- SUID - разрешение на установку идентификатора пользователя. Это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла.
- SGID - разрешение на установку идентификатора группы. Принцип работы очень похож на SUID с отличием, что файл будет запускаться пользователем от имени группы, которая владеет файлом.


## Цель лабораторной работы

Изучение механизмов изменения идентификаторов, применения SetUID и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# **Выполнение лабораторной работы**

---

# Программа simpleid

A terminal window with a dark background. The prompt is [guest@omgagloev ~]. The first command is gcc simpleid.c -o simpleid. The second command is ./simpleid. The output is uid=1001, gid=1001. The prompt returns to [guest@omgagloev ~].

```
[guest@omgagloev ~]$ gcc simpleid.c -o simpleid
[guest@omgagloev ~]$ ./simpleid
uid=1001, gid=1001
[guest@omgagloev ~]$
```

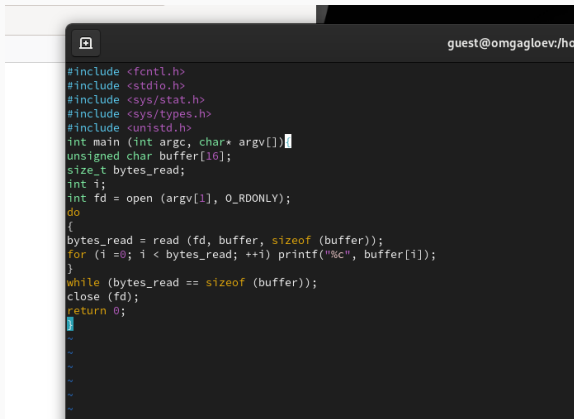
**Рис. 1:** Результат выполнения программы

# Программа simpleid2

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

Рис. 2: результат программы simpleid2

# Программа readfile



```
guest@omgagloev:/ho
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>
int main (int argc, char* argv[]) {
    unsigned char buffer[16];
    size_t bytes_read;
    int i;
    int fd = open (argv[1], O_RDONLY);
    do
    {
        bytes_read = read (fd, buffer, sizeof (buffer));
        for (i = 0; i < bytes_read; ++i) printf("%c", buffer[i]);
    }
    while (bytes_read == sizeof (buffer));
    close (fd);
    return 0;
}
```

**Рис. 3:** код программы readfile



# Программа readfile

```
[root@omgagloes guest]# ./readfile /etc/shadow
root:$6$uGFlydw/8x2AFvq9$sz1ICs492EHie8WxNzrzrV5vn0zIL8hVuG0g6ztf/DMSfkpynPk1JZs5FJKI19ZrQkvP0SbgUGZD.1vQt/::0:99999:7:::
bin:!:19469:0:99999:7:::
daemon:!:19469:0:99999:7:::
adm:!:19469:0:99999:7:::
lp:!:19469:0:99999:7:::
sync:!:19469:0:99999:7:::
80 shutdown:!:19469:0:99999:7:::
100 halt:!:19469:0:99999:7:::
mail:!:19469:0:99999:7:::
pc operator:!:19469:0:99999:7:::
10 games:!:19469:0:99999:7:::
101 ftp:!:19469:0:99999:7:::
nobody:!:19469:0:99999:7:::
111 systemd-coredump:!!!19609:!!!!:
112 dbus:!!!19609:!!!!:
113 polkitd:!!!19609:!!!!:
avahi:!!!19609:!!!!:
rkt:!!!19609:!!!!:
sssd:!!!19609:!!!!:
pipewire:!!!19609:!!!!:
libstoragemgmt:(!:19609:!!!!:
systemd-oom:!:19609:!!!!:
```

Рис. 4: Чтение с помощью readfile

# Проверка sticky бита

```
guest@omgagloev:/home/guest
[guest@omgagloev ~]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 Oct  6 17:54 tmp
[guest@omgagloev ~]$ echo "test" > /tmp/file01.txt
[guest@omgagloev ~]$ ls -l /tmp/file01.txt
chmod o+rw /tmp/file01.txt
ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  6 17:58 /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  6 17:58 /tmp/file01.txt
[guest@omgagloev ~]$
```

Рис. 5: Проверка sticky бита

# Проверка sticky бита

```
bash: /tmp/file01.txt: Permission denied
[guest2@omgagloev ~]$ cat /tmp/file01.txt
test
[guest2@omgagloev ~]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@omgagloev ~]$ cat /tmp/file01.txt
test
[guest2@omgagloev ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@omgagloev ~]$
```

Рис. 6: Работа с файлом

# Проверка sticky бита

```
5y drwxrwxrwx. 19 root root 4096 Oct 6 18:05 tmp
[root@omgagloev ~]# chmod +t /tmp
[root@omgagloev ~]# exit
logout
B [root@omgagloev guest]# ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 Oct 6 18:06 tmp
[root@omgagloev guest]#
```

Рис. 7: Возвращение sticky бита

## **Выводы**

---

Изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получили практические навыки работы в консоли с дополнительными атрибутами. Также мы рассмотрели работу механизма смены идентификатора процессов пользователей и влияние бита Sticky на запись и удаление файлов.