

## Лабораторная работа №5.

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

---

Стариков Данила Андреевич

13 апреля 2024

## Цели и задачи

---

- 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

## Результаты

---

```
#include<sys/types.h>
#include<unistd.h>
#include<stdio.h>

int main(){
    uid_t uid = geteuid();
    gid_t gid = getegid();
    printf("uid=%d, gid=%d\n", uid, gid);
    return 0;
}
```

```
[guest@dastarikov ~]$ ./simpleid
uid=1001, gid=1001
[guest@dastarikov ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@dastarikov ~]$
```

Рис. 1: Сравнение выводов программ id и simpleid.

```
#include<sys/types.h>
```

```
#include<unistd.h>
```

```
#include<stdio.h>
```

```
int main(){
```

```
    uid_t real_uid = getuid();
```

```
    uid_t e_uid = geteuid();
```

```
    gid_t real_gid = getgid();
```

```
    gid_t e_gid = getegid() ;
```

```
    printf("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
```

```
    printf("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
```

```
    return 0;
```

```
}
```

```
[guest@dastarikov ~]$ su -  
Password:  
[root@dastarikov ~]# chown root:guest /home/guest/simpleid2  
[root@dastarikov ~]# chmod u+s /home/guest/simpleid2  
[root@dastarikov ~]#  
logout  
[guest@dastarikov ~]$ ls -l simpleid2  
-rwsr-xr-x. 1 root guest 26064 Apr 13 19:49 simpleid2  
[guest@dastarikov ~]$
```

Рис. 2: Изменение владельца файла simpleid2 и добавление SUID-бита.



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

Рис. 3: Сравнение выводов программ id и simpleid2.

```
[guest@dastarikov ~]$ su -  
Password:  
[root@dastarikov ~]# chmod u-s /home/guest/simpleid2  
[root@dastarikov ~]# chmod g+s /home/guest/simpleid2  
[root@dastarikov ~]#  
logout  
[guest@dastarikov ~]$ ls -l simpleid2  
-rwxr-sr-x. 1 root guest 26064 Apr 13 19:49 simpleid2  
[guest@dastarikov ~]$
```

Рис. 4: Изменение группы-владельца файла simpleid2 и добавление GUID-бита.

```
[root@dastarikov ~]# chmod g+s /home/guest/simpleid2
[root@dastarikov ~]# ls -l /home/guest/simpleid2
-rwxr-sr-x. 1 root root 26064 Apr 13 19:49 /home/guest/simpleid2
[root@dastarikov ~]#
logout
[guest@dastarikov ~]$ ./simpleid2
e_uid=1001, e_gid=0
real_uid=1001, real_gid=1001
[guest@dastarikov ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@dastarikov ~]$
```

Рис. 5: Сравнение выводов программ id и simpleid2 для SGID-бита.

```
#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 fd = open(argv[1], O_RDONLY);
    do{ bytes_read = read(fd, buffer, sizeof (buffer));
    for (int i=0;i<bytes_read;++i) printf("%c", buffer[i]);
    } while (bytes_read == sizeof(buffer));
    close(fd);
    return 0;}
```

```
[guest@dastarikov ~]$ su -  
Password:  
[root@dastarikov ~]# chown root:root /home/guest/readfile.c  
[root@dastarikov ~]# chmod 770 /home/guest/readfile.c  
[root@dastarikov ~]# ls -l /home/guest/readfile.c  
-rwxrwx---. 1 root root 398 Apr 13 20:15 /home/guest/readfile.c  
[root@dastarikov ~]#  
logout  
[guest@dastarikov ~]$ cat readfile.c  
cat: readfile.c: Permission denied  
[guest@dastarikov ~]$
```

Рис. 6: Изменение прав файла readfile.c и проверка изменений.

```
[guest@dastarikov ~]$ su -
Password:
[root@dastarikov ~]# chown root /home/guest/readfile
[root@dastarikov ~]# chmod u+s /home/guest/readfile
[root@dastarikov ~]# ls -l /home/guest/readfile
-rwsr-xr-x. 1 root guest 26008 Apr 13 20:15 /home/guest/readfile
[root@dastarikov ~]#
logout
[guest@dastarikov ~]$ ./readfile readfile.c
#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;
}
[guest@dastarikov ~]$
```

```
[guest@dastarikov ~]$ ./readfile /etc/shadow
root:$6$dz/KFZWdA5GU.9ho$LJyGhWIh98pg4LNacTwZr7seaDuS1fkUBuYkn5ohDnMz59jZIBw5/1rLGkYE7fEu
7oLMQgZqpK0PUZeKfRpbo0::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:::
shutdown:*:19469:0:99999:7:::
halt:*:19469:0:99999:7:::
```

Рис. 8: Сравнение выводов программ id и simpleid2 для SGID-бита.

```
[guest@dastarikov ~]$ ls -l / | grep tmp  
drwxrwxrwt. 15 root root 4096 Apr 13 20:24 tmp  
[guest@dastarikov ~]$
```

Рис. 9: Проверка атрибута Sticky на /tmp.



```
[guest@dastarikov ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Apr 13 20:27 /tmp/file01.txt
[guest@dastarikov ~]$ echo "test" > /tmp/file01.txt
[guest@dastarikov ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Apr 13 20:27 /tmp/file01.txt
[guest@dastarikov ~]$ chmod o+rw /tmp/file01.txt
[guest@dastarikov ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Apr 13 20:27 /tmp/file01.txt
```

Рис. 10: Изменение атрибутов файла file01.txt.

```
[guest@dastarikov ~]$ su guest2
Password:
[guest2@dastarikov guest]$ cat /tmp/file01.txt
test
[guest2@dastarikov guest]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@dastarikov guest]$ cat /tmp/file01.txt
test
[guest2@dastarikov guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@dastarikov guest]$ cat /tmp/file01.txt
test
[guest2@dastarikov guest]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@dastarikov guest]$
```

Рис. 11: Проверка прав работы с file01.txt у невладельца файла (guest2).

```
[guest2@dastarikov guest]$ su -  
Password:  
[root@dastarikov ~]# chmod -t /tmp  
[root@dastarikov ~]#  
logout  
[guest2@dastarikov guest]$ ls -l | grep tmp  
[guest2@dastarikov guest]$ ls -l | grep /tmp  
[guest2@dastarikov guest]$ ls -l / | grep tmp  
drwxrwxrwx. 15 root root 4096 Apr 13 20:32 tmp  
[guest2@dastarikov guest]$
```

Рис. 12: Снятие Sticky-бита с /tmp.

```
[guest2@dastarikov guest]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@dastarikov guest]$ cat /tmp/file01.txt
test
[guest2@dastarikov guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@dastarikov guest]$ cat /tmp/file01.txt
test
[guest2@dastarikov guest]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@dastarikov guest]$ cat /tmp/file01.txt
cat: /tmp/file01.txt: No such file or directory
```

Рис. 13: Проверка прав работы с file01.txt у невладельца файла (guest2) без Sticky-бита.

ИТОГ



- В рамках лабораторной работы изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов, Получили практические навыки работы в консоли с дополнительными атрибутами. Рассмотрели работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.