## Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Хусайнова Фароиз НКНбд-01-181

13 ноября 2021 г., Москва, Россия

<sup>1</sup>российский Университет Дружбы Народов

## 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.



```
[guest0mona ~1$ gcc simpleid.c
[guest0mona ~1$ gcc simpleid.c -o simpleid
[guest0mona ~1$ ./simpleid
uid=1001, gid=1001
[guest0mona ~1$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0
-s0:c0.c1023
[guest0mona ~1$ _
```

Figure 1: результат программы simpleid

```
[guest0mona ~1$ gcc simpleid2.c
[guest@mona ~1$ gcc simpleid2.c -o simpleid2
[guest@mona ~1$ ./simpleid2
e_uid=1001, e_qid=1001
real_uid=1001, real_gid=1001
Iguest@mona ~1$ su
Password:
[root@mona guest]# chown root:guest simpleid2
[root@mona guest]# chmod u+s simpleid2
[root@mona quest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@mona guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@mona guest]# chmod g+s simpleid2
[root@mona guest]# ls -l simpleid2
-rwsrwsr-x. 1 root guest 8576 Nov 13 17:42 simpleid2
[root@mona guest]# ./simpleid2
e_uid=0, e_qid=1001
real_uid=0, real_gid=0
[root@mona guest]# exit
exit
[guest@mona ~1$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@mona ~1$ _
```

Figure 2: результат программы simpleid2

```
[guest@mona ~1$ cat 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("xc", buffer[i]);
  while (bytes_read == sizeof (buffer));
  close (fd);
  return 0;
[guest@mona ~]$ ./readfile /etc/shadow
UXUUXUUXUUXUUXUXUXU!PXUUdQQ8 PLU
                                     ∎é9Ű|þŸí¿|þŸI∎x∎=eU∎
                 UDDPDDWX86_64./readfile/etc/shadowXDG_VTNR=1XDG_SESSION_ID=1HOSTNAME=mona.local
domainSHELL=/bin/bashTERM=linuxHISTSIZE=1000USER=guestLS_COLORS=rs=0:di=01:34:ln=01;36:mh=00:pi=40;3
3:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=01;05;37;41:su=37;41:sg=30;43:ca=30;41:tu
=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.ar_j=01;31:*.taz=01;31:*.lha:
01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01Segmentation fault
[guest@mona ~1$ _
```

Figure 3: результат программы readfile

```
[guest0mona ~1$ ls -l / i grep tmp
drworworwt. 7 root root 111 Nov 13 17:42 tmp
[guest0mona ~1$ echo "test" > /tmp/file01.txt
[guest0mona ~1$ ls -l /tmp/file01.txt
[guest0mona ~1$ ls -l /tmp/file01.txt
[guest0mona ~1$ chmod o+pw /tmp/file01.txt
[guest0mona ~1$ ls -l /tmpfile01.txt
[guest0mona ~1$ ls -l /tmpfile01.txt
[s: cannot access /tmpfile01.txt: No such file or directory
[guest0mona ~1$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Nov 13 18:89 /tmp/file01.txt
[guest0mona ~1$ ls -l /tmp/file01.txt
```

```
uest20mona guest1$ cat /tmp/file01.txt
[guest2@mona guest]$ echo "test3" > /tmp/file01.txt
[guest2@mona guest]$ cat /tmp/file01.txt
[guest20mona guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
quest20mona quest1$ su
assword:
[root@mona guest]# chmod -t /tmp
[root@mona guest]# exit
[guest2@mona guest]$ ls −l / grep tmp
 : cannot access grep: No such file or directory
: cannot access tmp: No such file or directory
total 16
lrwxrwxrwx. 1 root root 7 Sep 18 20:37 bin -> usr/bin
dr-xr-xr-x. 5 root root 4096 Sep 18 21:21 boot
lrwxr-xr-x. 20 root root 3080 Nov 13 15:34 dev
lrwxr-xr-x. 74 root root 8192 Nov 13 15:34 etc
drwxr-xr-x. 6 root root 64 Oct 30 16:07 home
lruxruxrux. 1 root root 7 Sep 18 20:37 lib → usr/lib
rwxrwxrwx. 1 root root 9 Sep 18 20:37 lib64 -> usr/lib64
lrwxr-xr-x. Z root root 6 Apr 11 2018 media
drwxr-xr-x. 2 root root 6 Apr 11 2018 mnt
lrwxr-xr-x. Z root root 6 Apr 11 2018 opt
r-xr-xr-x. 113 root root 0 Nov 13 15:33 proc
r-xr-x---. 2 root root 135 Nov 13 16:44 root
rwxr-xr-x. 23 root root 700 Nov 13 15:34 run
rwxrwxrwx. 1 root root 8 Sep 18 20:37 sbin -> usr/sbin
rwxr-xr-x. 2 root root 6 Apr 11 2018 srv
lr-xr-xr-x. 13 root root 0 Nov 13 15:33 sys
drwxrwxrwx. 7 root root 111 Nov 13 17:16 🧰
drwxr-xr-x. 13 root root 155 Sep 18 20:37 <mark>usr</mark>
lrwxr-xr-x. 19 root root 267 Sep 18 21:25 var
guest20mona guest1$
```

```
[guest20mona guest]$ su -
Password:
Last login: Sat Nov 13 17:24:46 MSK 2021 on tty1
[root0mona ~]# chmod +t /tmp
[root0mona ~]# exit
logout
```

Figure 3: Исследование 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.