

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Альсид Мона НФИбд-03-18¹

13 ноября 2021 г., Москва, Россия

¹российский 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.

Выполнения лабораторной работы

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

Figure 1: результат программы simpleid

```
[guest@mona ~]$ gcc simpleid2.c
[guest@mona ~]$ gcc simpleid2.c -o simpleid2
[guest@mona ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@mona ~]$ su
Password:
[root@mona guest]$ chown root:guest simpleid2
[root@mona guest]$ chmod u+s simpleid2
[root@mona guest]$ ./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_gid=1001
real_uid=0, real_gid=0
[root@mona guest]$ exit
exit
[guest@mona ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@mona ~]$ _
```

Figure 2 : результат программы simpleid2

```
lguest@mona ~]$ 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("%c", buffer[i]);
    }

    while (bytes_read == sizeof (buffer));
    close (fd);
    return 0;
}

lguest@mona ~]$ ./readfile /etc/shadow
0Ry0Nc 00xR10Rc/cGc 00xI0(xxxxxxxx xxxxxxxxxx xxxxxxxxxx xxxxxxxxxx 0x0x0xQxhxxy
xxxxxxx xxxxxx!Pxddd008 PL  0
é9Ü|pYí¿|pYIxx=eU
UppWx86_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:tw
=30:42:ow=34:42:st=37:44:ex=01:32:*.tar=01:31:*.tgz=01:31:*.arc=01:31:*.arj=01:31:*.taz=01:31:*.lha=
01:31:*.lz4=01:31:*.lzh=01:31:*.lzma=01:31:*.tlz=01Segmentation fault
lguest@mona ~]$ _
```

Figure 3: результат программы readfile

```

[guest@mona ~]$ ls -l / | grep tmp
drwxrwxrwt.  7 root root  111 Nov 13 17:42 tmp
[guest@mona ~]$ echo "test" > /tmp/file01.txt
[guest@mona ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Nov 13 18:09 /tmp/file01.txt
[guest@mona ~]$ chmod o+rw /tmp/file01.txt
[guest@mona ~]$ ls -l /tmpfile01.txt
ls: cannot access /tmpfile01.txt: No such file or directory
[guest@mona ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Nov 13 18:09 /tmp/file01.txt
[guest@mona ~]$

```

```

[guest2@mona guest]$ cat /tmp/file01.txt
test2
[guest2@mona guest]$ echo "test3" > /tmp/file01.txt
[guest2@mona guest]$ cat /tmp/file01.txt
test3
[guest2@mona guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@mona guest]$ su
Password:
[root@mona guest]# chmod -t /tmp
[root@mona guest]# exit
exit
[guest2@mona guest]$ ls -l / grep tmp
ls: cannot access grep: No such file or directory
ls: cannot access tmp: No such file or directory
/
total 16
drwxrwxrwx.  1 root root   7 Sep 18 20:37 bin -> usr/bin
dr-xr-xr-x.  5 root root 4096 Sep 18 21:21 boot
drwxr-xr-x. 20 root root 3080 Nov 13 15:34 dev
drwxr-xr-x. 74 root root 8192 Nov 13 15:34 etc
drwxr-xr-x.  6 root root  64 Oct 30 16:07 home
drwxrwxrwx.  1 root root   7 Sep 18 20:37 lib -> usr/lib
drwxrwxrwx.  1 root root   9 Sep 18 20:37 lib64 -> usr/lib64
drwxr-xr-x.  2 root root   6 Apr 11  2018 media
drwxr-xr-x.  2 root root   6 Apr 11  2018 mnt
drwxr-xr-x.  2 root root   6 Apr 11  2018 opt
dr-xr-xr-x. 113 root root   0 Nov 13 15:33 proc
dr-xr-xr-x.  2 root root 135 Nov 13 16:44 root
drwxr-xr-x. 23 root root 780 Nov 13 15:34 run
drwxrwxrwx.  1 root root   8 Sep 18 20:37/sbin -> usr/sbin
drwxr-xr-x.  2 root root   6 Apr 11  2018 srv
dr-xr-xr-x. 13 root root   0 Nov 13 15:33 sys
drwxrwxrwx.  7 root root  11 Nov 13 17:16 tmp
drwxr-xr-x. 13 root root 155 Sep 18 20:37 usr
drwxr-xr-x. 19 root root 267 Sep 18 21:25 var
[guest2@mona guest]$ _

```

```

[guest2@mona guest]$ su -
Password:
Last login: Sat Nov 13 17:24:46 MSK 2021 on tty1
[root@mona ~]# chmod +t /tmp
[root@mona ~]# exit
Input

```

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.