

Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Липатникова Марина Сергеевна

08.10.2022, Moscow

RUDN University, Moscow, Russian Federation

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

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

Figure 1: Работа с программой simpleid

Выполнение лабораторной работы

```
[guest@mslipatnikova ~]$ nano simpleid.c
[guest@mslipatnikova ~]$ ls
Desktop  Documents  Music      Public    simpleid2.c  Templates
dir1     Downloads  Pictures   simpleid  simpleid.c   Videos
[guest@mslipatnikova ~]$ cat simpleid2.c
#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 ("uid=%d, gid=%d\n",e_uid,e_gid);
    printf ("real_uid=%d,real_gid=%d\n", real_uid, real_gid);
    return 0;
}
[guest@mslipatnikova ~]$ gcc simpleid2.c -o simpleid2
[guest@mslipatnikova ~]$ ./simpleid2
uid=1001, gid=1001
real_uid=1001,real_gid=1001
```

Figure 2: Работа с программой simpleid2

Выполнение лабораторной работы

```
[guest@mslipatnikova ~]$ ls -l simpleid2
-rwxrwxr-x. 1 root guest 26008 Oct 8 16:21 simpleid2
[guest@mslipatnikova ~]$ ./simpleid2
uid=0, gid=1001
real uid=1001, real gid=1001
[guest@mslipatnikova ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
```

Figure 3: Работа simpleid2(u+s)

```
[guest@mslipatnikova ~]$ ls -l simpleid2
-rwxrwxr-x. 1 root guest 26008 Oct 8 16:21 simpleid2
[guest@mslipatnikova ~]$ ./simpleid2
uid=0, gid=1001
real uid=1001, real gid=1001
[guest@mslipatnikova ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
```

Figure 4: Работа simpleid2(g+s)

```
[root@mslipatnikova ~]# chown root:guest /home/guest/simpleid2
[root@mslipatnikova ~]# chmod u+s /home/guest/simpleid2
[root@mslipatnikova ~]# chmod g+s /home/guest/simpleid2
```

Figure 5: Команды от суперпользователя

```
[quest@mslipatnikova ~]$ touch readfile.c
[quest@mslipatnikova ~]$ nano readfile.c
[quest@mslipatnikova ~]$ 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;
}
[quest@mslipatnikova ~]$ gcc readfile.c -o readfile
```

Figure 6: Программа readfile

```
[guest@mslipatnikova ~]$ ls -l readfile.c
-rwx-----. 1 root guest 418 Oct  8 17:10 readfile.c
[guest@mslipatnikova ~]$ cat readfile.c
cat: readfile.c: Permission denied
```

Figure 7: Чтение readfile.c

```
[root@mslipatnikova ~]# chown root /home/guest/readfile.c
[root@mslipatnikova ~]# chmod 700 /home/guest/readfile.c
[root@mslipatnikova ~]# chown root:guest /home/guest/readfile
[root@mslipatnikova ~]# chmod u+s /home/guest/readfile
[root@mslipatnikova ~]# chmod g+s /home/guest/readfile
```

Figure 8: Команды от суперпользователя

Выполнение лабораторной работы

```
[quest@mslapnikova ~]$ ./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[10];
    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;
}

[quest@mslapnikova ~]$ ./readfile /etc/shadow
root:$6$me4c/r99wllhsc1b4axcfcxf1fg0wu0/d7udqkq5VPcQX5X5US4K121v10wmy0t0v
0r557f8A0u0j0t7r0e25527353h0tby1:0:99999:7:::
bin:!:19123:0:99999:7:::
daemon:!:19123:0:99999:7:::
adm:!:19123:0:99999:7:::
lp:!:19123:0:99999:7:::
sync:!:19123:0:99999:7:::
shutdown:!:19123:0:99999:7:::
halt:!:19123:0:99999:7:::
mail:!:19123:0:99999:7:::
operator:!:19123:0:99999:7:::
games:!:19123:0:99999:7:::
ftp:!:19123:0:99999:7:::
nobody:!:19123:0:99999:7:::
systemd-coredump:!:19242:!!!!:
dbus:!:19242:!!!!:
polkitd:!:19242:!!!!:
rtkit:!:19242:!!!!:
sssd:!:19242:!!!!:
avahi:!:19242:!!!!:
pipewire:!:19242:!!!!:
libstoragemgmt:!:19242:!!!!:
tss:!:19242:!!!!:
```

Figure 9: Чтение с помощью программы readfile


```
[guest@mslipatnikova ~]$ ls -l / | grep tmp
drwxrwxrwt. 16 root root 4096 Oct  8 17:10 tmp
[guest@mslipatnikova ~]$ echo "test" > /tmp/file01.txt
[guest@mslipatnikova ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 Oct  8 17:18 /tmp/file01.txt
[guest@mslipatnikova ~]$ chmod o+rw /tmp/file01.txt
[guest@mslipatnikova ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 Oct  8 17:18 /tmp/file01.txt
[guest@mslipatnikova ~]$ su guest2
Password:
[guest2@mslipatnikova guest]$ echo "test2">>/tmp/file01.txt
[guest2@mslipatnikova guest]$ cat /tmp/file01.txt
test
test2
[guest2@mslipatnikova guest]$ echo "test3">/tmp/file01.txt
[guest2@mslipatnikova guest]$ cat /tmp/file01.txt
test3
[guest2@mslipatnikova guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
```

Figure 10: Работа с tmp/file01.txt

```
[guest2@mslipatnikova guest]$ ls -l / | grep tmp
drwxrwxrwx. 16 root root 4096 Oct  8 17:23 tmp
[guest2@mslipatnikova guest]$ echo "test2">>/tmp/file01.txt
[guest2@mslipatnikova guest]$ cat /tmp/file01.txt
test3
test2
[guest2@mslipatnikova guest]$ echo "test3">/tmp/file01.txt
[guest2@mslipatnikova guest]$ cat /tmp/file01.txt
test3
[guest2@mslipatnikova guest]$ rm /tmp/file01.txt
```

Figure 11: Работа с tmp/file01.txt без t

```
[root@mslipatnikova ~]# chmod -t /tmp
[root@mslipatnikova ~]# chmod +t /tmp
```

Figure 12: Команды от суперпользователя

Изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получила практические навыки работы в консоли с дополнительными атрибутами. Рассмотрела работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

1. Теоретические материалы курса.