

Презентация лабораторной работы №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Тасыбаева Н.С.

7 октября 2023

Российский университет дружбы народов, Москва, Россия

Цели и задачи 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.

```
[guest@nstasihbaeva ~]$ mkdir lab5
[guest@nstasihbaeva ~]$ ls -l lab5
total 0
[guest@nstasihbaeva ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 16 17:44 Desktop
drwxrwxrwx. 2 guest guest 19 Sep 30 18:39 lib
drwxr-xr-x. 2 guest guest 6 Sep 16 17:44 Documents
drwxr-xr-x. 2 guest guest 6 Sep 16 17:44 Downloads
drwxr-xr-x. 2 guest guest 6 Oct 7 17:43 lab5
drwxr-xr-x. 2 guest guest 6 Sep 16 17:44 Music
drwxr-xr-x. 2 guest guest 53 Sep 16 17:51 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 16 17:44 Public
drwxr-xr-x. 2 guest guest 6 Sep 16 17:44 Templates
drwxr-xr-x. 2 guest guest 6 Sep 16 17:44 Videos
[guest@nstasihbaeva ~]$ cd lab5
[guest@nstasihbaeva lab5]$ touch simpleid.c
[guest@nstasihbaeva lab5]$ vi simpleid.c
[guest@nstasihbaeva lab5]$ 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@nstasihbaeva lab5]$ gcc simpleid.c -o simpleid
[guest@nstasihbaeva lab5]$ ./simpleid
uid=1001, gid=1001
[guest@nstasihbaeva lab5]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@nstasihbaeva lab5]$
```

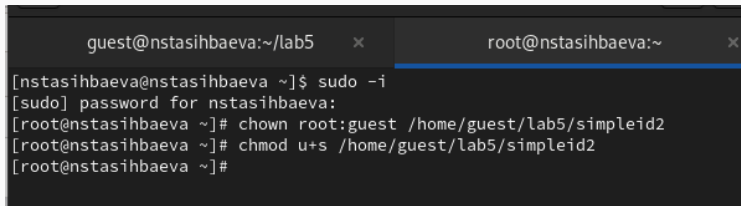
Рис. 1: Создание и запуск simpleid.c

```
[guest@nstasihbaeva lab5]$ gcc simpleid.c -o simpleid
[guest@nstasihbaeva lab5]$ 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 ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
    printf ("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
}

[guest@nstasihbaeva lab5]$ gcc simpleid2.c -o simpleid2
[guest@nstasihbaeva lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@nstasihbaeva lab5]$
```

Рис. 2: Создание и запуск simpleid2.c



The image shows a terminal window with two tabs. The first tab is titled 'guest@nstasihbaeva:~/lab5' and the second, active tab is titled 'root@nstasihbaeva:~'. The terminal history shows a user running 'sudo -i' to become root, followed by 'chown root:guest /home/guest/lab5/simpleid2' and 'chmod u+s /home/guest/lab5/simpleid2' to change permissions.

```
guest@nstasihbaeva:~/lab5  ×    root@nstasihbaeva:~  ×
[nstasihbaeva@nstasihbaeva ~]$ sudo -i
[sudo] password for nstasihbaeva:
[root@nstasihbaeva ~]# chown root:guest /home/guest/lab5/simpleid2
[root@nstasihbaeva ~]# chmod u+s /home/guest/lab5/simpleid2
[root@nstasihbaeva ~]#
```

Рис. 3: Смена владельца и изменение прав на файл simpleid2.c

```
[guest@nstasihbaeva lab5]$ ls -l simpleid2
-rwsr-xr-x. 1 root guest 26064 Oct  7 17:56 simpleid2
[guest@nstasihbaeva lab5]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@nstasihbaeva lab5]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 4: Запуск simpleid2 после смены владельца и прав

```
[root@nstashbaeva ~]# chmod g+s /home/guest/lab5/simpleid2  
[root@nstashbaeva ~]#
```

Рис. 5: Смена прав относительно SetGID-бита


```
[guest@nstasihbaeva lab5]$ ls -l simpleid2
-rwsr-sr-x. 1 root guest 26064 Oct  7 17:56 simpleid2
[guest@nstasihbaeva lab5]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@nstasihbaeva lab5]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_
t:s0-s0:c0.c1023
[guest@nstasihbaeva lab5]$
```

Рис. 6: Повторение команд

[illegible]

Рис. 7: Выполнение команд для readfile

```
[guest@nstashbaeva ~]$ ls -l / | grep tmp
drwxrwxrwt. 18 root root 4096 Oct 7 18:42 tmp
[guest@nstashbaeva ~]$ echo "test" > /tmp/file01.txt
[guest@nstashbaeva ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct 7 18:44 /tmp/file01.txt
[guest@nstashbaeva ~]$ chmod o+rw /tmp/file01.txt
[guest@nstashbaeva ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct 7 18:44 /tmp/file01.txt
[guest@nstashbaeva ~]$ cat /tmp/file01.txt
test
[guest@nstashbaeva ~]$ su guest2
Password:
su: Authentication failure
[guest@nstashbaeva ~]$ su guest2
Password:
[guest2@nstashbaeva guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@nstashbaeva guest]$ cat /tmp/file01.txt
test
[guest2@nstashbaeva guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@nstashbaeva guest]$ cat /tmp/file01.txt
test
[guest2@nstashbaeva 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@nstashbaeva guest]$ su -
Password:
[root@nstashbaeva ~]# chmod -t /tmp
[root@nstashbaeva ~]# exit
logout
[guest2@nstashbaeva guest]$ ls -l / | grep tmp
drwxrwxrwt. 18 root root 4096 Oct 7 18:51 tmp
[guest2@nstashbaeva guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@nstashbaeva guest]$ cat /tmp/file01.txt
test
[guest2@nstashbaeva guest]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@nstashbaeva guest]$ ls -l /tmp
total 28
drwx-----. 3 root      root      17 Oct 7 16:58 systemd-private-c29e8919cab3438cab8ed9a2476f6ba2-chromyd.service-Tuk9L3
drwx-----. 3 root      root      17 Oct 7 17:00 systemd-private-c29e8919cab3438cab8ed9a2476f6ba2-color.service-wDzvd
drwx-----. 3 root      root      17 Oct 7 16:58 systemd-private-c29e8919cab3438cab8ed9a2476f6ba2-dbus-broker.service-C3jshb
drwx-----. 3 root      root      17 Oct 7 17:22 systemd-private-c29e8919cab3438cab8ed9a2476f6ba2-fuupd.service-avL201
drwx-----. 3 root      root      17 Oct 7 17:22 systemd-private-c29e8919cab3438cab8ed9a2476f6ba2-guac.service-r2W80V
drwx-----. 3 root      root      17 Oct 7 16:58 systemd-private-c29e8919cab3438cab8ed9a2476f6ba2-guac.service-r2W80V
```

Рис. 8: Выполнение команд

```
vboxguest-Module.symvers
[guest2@nstashbaeva guest]$ su -
Password:
[root@nstashbaeva ~]# chmod +t /tmp
[root@nstashbaeva ~]# exit
logout
[guest2@nstashbaeva guest]$ ls -l / | grep tmp
drwxrwxrwt. 20 root root 4096 Oct  7 18:55 tmp
[guest2@nstashbaeva guest]$
```

Рис. 9: Выполнение команд

Выводы по проделанной работе

Я 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.