

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Боровиков Даниил Александрович

13 апреля, 2024, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

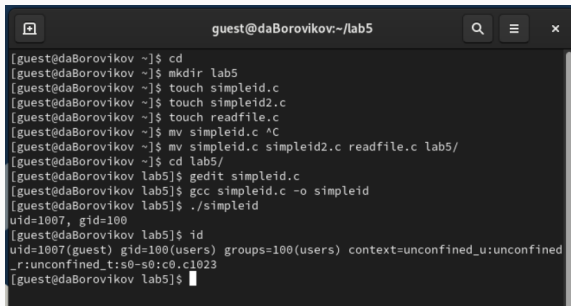
- SUID - разрешение на установку идентификатора пользователя. Это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла.
- SGID - разрешение на установку идентификатора группы. Принцип работы очень похож на SUID с отличием, что файл будет запускаться пользователем от имени группы, которая владеет файлом.

Цель лабораторной 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.

Выполнение лабораторной работы

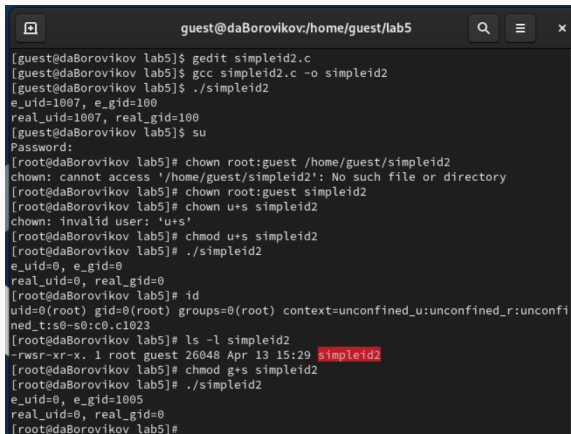
Программа simpleid



```
guest@daBorovikov:~/lab5
[guest@daBorovikov ~]$ cd
[guest@daBorovikov ~]$ mkdir lab5
[guest@daBorovikov ~]$ touch simpleid.c
[guest@daBorovikov ~]$ touch simpleid2.c
[guest@daBorovikov ~]$ touch readfile.c
[guest@daBorovikov ~]$ mv simpleid.c ^C
[guest@daBorovikov ~]$ mv simpleid.c simpleid2.c readfile.c lab5/
[guest@daBorovikov ~]$ cd lab5/
[guest@daBorovikov lab5]$ gedit simpleid.c
[guest@daBorovikov lab5]$ gcc simpleid.c -o simpleid
[guest@daBorovikov lab5]$ ./simpleid
uid=1007, gid=100
[guest@daBorovikov lab5]$ id
uid=1007(guest) gid=100(users) groups=100(users) context=unconfined_u:unconfined
_r:unconfined_t:s0-s0:c0.c1023
[guest@daBorovikov lab5]$
```

Figure 1: результат программы simpleid

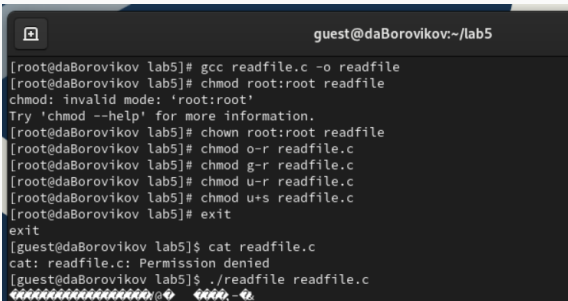
Программа simpleid2



```
guest@daBorovikov:/home/guest/lab5
[guest@daBorovikov lab5]$ gedit simpleid2.c
[guest@daBorovikov lab5]$ gcc simpleid2.c -o simpleid2
[guest@daBorovikov lab5]$ ./simpleid2
e_uid=1007, e_gid=100
real_uid=1007, real_gid=100
[guest@daBorovikov lab5]$ su
Password:
[root@daBorovikov lab5]# chown root:guest /home/guest/simpleid2
chown: cannot access '/home/guest/simpleid2': No such file or directory
[root@daBorovikov lab5]# chown root:guest simpleid2
[root@daBorovikov lab5]# chown u+s simpleid2
chown: invalid user: 'u+s'
[root@daBorovikov lab5]# chmod u+s simpleid2
[root@daBorovikov lab5]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@daBorovikov lab5]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfi
ned_t:s0-s0:c0.c1023
[root@daBorovikov lab5]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 26048 Apr 13 15:29 simpleid2
[root@daBorovikov lab5]# chmod g+s simpleid2
[root@daBorovikov lab5]# ./simpleid2
e_uid=0, e_gid=1005
real_uid=0, real_gid=0
[root@daBorovikov lab5]#
```

Figure 2: результат программы simpleid2

Программа readfile

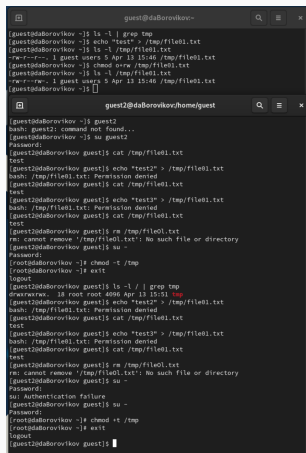
A terminal window with a dark background. The title bar shows a window icon and the text "guest@daBorovikov:~/lab5". The terminal content shows a series of commands and their outputs. The user is initially root@daBorovikov lab5. They compile readfile.c to readfile, attempt to set permissions to root:root (which fails), then use chown to set root:root. They then set permissions to o-r, g-r, u-r, and u+s. Finally, they exit root and run the program as guest@daBorovikov lab5. The program attempts to cat readfile.c but is denied permission. The prompt then changes to a decorative pattern.

```
guest@daBorovikov:~/lab5

[root@daBorovikov lab5]# gcc readfile.c -o readfile
[root@daBorovikov lab5]# chmod root:root readfile
chmod: invalid mode: 'root:root'
Try 'chmod --help' for more information.
[root@daBorovikov lab5]# chown root:root readfile
[root@daBorovikov lab5]# chmod o-r readfile.c
[root@daBorovikov lab5]# chmod g-r readfile.c
[root@daBorovikov lab5]# chmod u-r readfile.c
[root@daBorovikov lab5]# chmod u+s readfile.c
[root@daBorovikov lab5]# exit
exit
[guest@daBorovikov lab5]$ cat readfile.c
cat: readfile.c: Permission denied
[guest@daBorovikov lab5]$ ./readfile readfile.c
XXXXXXXXXXXXXXXXX@  XXXX,-X
```

Figure 3: результат программы readfile

Исследование Sticky-бита



```
guest@daBorovkov:~$ ls -l | grep tmp
-rw-r--r-- 1 guest users 5 Apr 13 15:46 /tmp/file01.txt
(guest@daBorovkov:~$ echo "test" > /tmp/file01.txt
(guest@daBorovkov:~$ ls -l /tmp/file01.txt
-rw-r--r-- 1 guest users 5 Apr 13 15:46 /tmp/file01.txt
(guest@daBorovkov:~$ chmod o=rw /tmp/file01.txt
-rw-r--r-- 1 guest users 5 Apr 13 15:46 /tmp/file01.txt
(guest@daBorovkov:~$

guest2@daBorovkov:~/home/guest$

(guest2@daBorovkov:~/home/guest$ guest2
bash: guest2: command not found...
(guest2@daBorovkov:~/home/guest$ su guest2
Password:
(guest2@daBorovkov:~/home/guest$ cat /tmp/file01.txt
test
(guest2@daBorovkov:~/home/guest$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
(guest2@daBorovkov:~/home/guest$ cat /tmp/file01.txt
test
(guest2@daBorovkov:~/home/guest$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
(guest2@daBorovkov:~/home/guest$ cat /tmp/file01.txt
test
(guest2@daBorovkov:~/home/guest$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
(guest2@daBorovkov:~/home/guest$ su -
Password:
(root@daBorovkov:~/home/guest$ chmod -t /tmp
logout
(guest2@daBorovkov:~/home/guest$ ls -l | grep tmp
drwxrwxr-x 18 root root 4096 Apr 13 15:51 tmp
(guest2@daBorovkov:~/home/guest$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
(guest2@daBorovkov:~/home/guest$ cat /tmp/file01.txt
test
(guest2@daBorovkov:~/home/guest$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
(guest2@daBorovkov:~/home/guest$ cat /tmp/file01.txt
test
(guest2@daBorovkov:~/home/guest$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
(guest2@daBorovkov:~/home/guest$ su -
Password:
su: Authentication failure
(guest2@daBorovkov:~/home/guest$ su -
Password:
(root@daBorovkov:~/home/guest$ chmod +t /tmp
(root@daBorovkov:~/home/guest$ exit
logout
(guest2@daBorovkov:~/home/guest$
```

Figure 4: 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.