Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Арутюнян Эрик

26 сентября, 2024, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Теоретическое введение

- 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

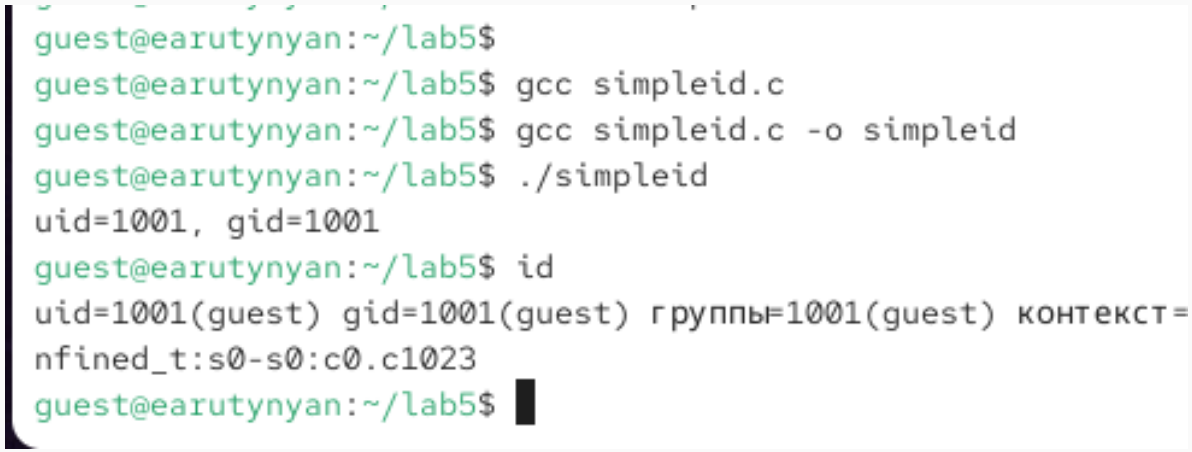

Рис. 1: результат программы simpleid

Программа simpleid2

```
guest@earutynyan:~/lab5$ gcc simpleid2.c
guest@earutynyan:~/lab5$ gcc simpleid2.c -o simpleid2
guest@earutynyan:~/lab5$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
guest@earutynyan:~/lab5$ su
Пароль:
root@earutynyan:/home/guest/lab5# chown root:guest simpleid2
root@earutynyan:/home/guest/lab5# chmod u+s simpleid2
root@earutynyan:/home/guest/lab5# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
root@earutynyan:/home/guest/lab5# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfinec
s0:c0.c1023
root@earutynyan:/home/guest/lab5# chmod g+s simpleid2
root@earutynyan:/home/guest/lab5# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
root@earutynyan:/home/guest/lab5#
exit
guest@earutynyan:~/lab5$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
guest@earutynyan:~/lab5$
```

Рис. 2: результат программы simpleid2

Программа readfile

```
guest@earutynyan:~/lab5$
guest@earutynyan:~/lab5$ touch readfile.c
guest@earutynyan:~/lab5$ gcc readfile.c
readfile.c: В функции «main»:
readfile.c:20:19: предупреждение: сравнение указателя и целого
   20 | while (bytes_read == (buffer));
      |                   ^~
guest@earutynyan:~/lab5$ gcc readfile.c -o readfile
readfile.c: В функции «main»:
readfile.c:20:19: предупреждение: сравнение указателя и целого
   20 | while (bytes_read == (buffer));
      |                   ^~
guest@earutynyan:~/lab5$ su
Пароль:
root@earutynyan:/home/guest/lab5# chown root:root readfile
root@earutynyan:/home/guest/lab5# chmod -rwx readfile.c
root@earutynyan:/home/guest/lab5# chmod u+s readfile
root@earutynyan:/home/guest/lab5#
exit
guest@earutynyan:~/lab5$ cat readfile.c
cat: readfile.c: Отказано в доступе
guest@earutynyan:~/lab5$ ./readfile readfile.c
#include <stdio.guest@earutynyan:~/lab5$
guest@earutynyan:~/lab5$ ./readfile /etc/shadow
root:$y$j9T$zlZFguest@earutynyan:~/lab5$
guest@earutynyan:~/lab5$
```

Рис. 3: результат программы readfile

Исследование Sticky-бита

```
guest@earutynyan:~/lab5$
guest@earutynyan:~/lab5$ echo "test" >> /tmp/file01.txt
guest@earutynyan:~/lab5$ chmod g+rwx /tmp/file01.txt
guest@earutynyan:~/lab5$ su guest2
Пароль:
guest2@earutynyan:/home/guest/lab5$ cd /tmp
guest2@earutynyan:/tmp$ cat file01.txt
test
guest2@earutynyan:/tmp$ echo "test2" >> /tmp/file01.txt
guest2@earutynyan:/tmp$ cat file01.txt
test
test2
guest2@earutynyan:/tmp$ echo "test3" > /tmp/file01.txt
guest2@earutynyan:/tmp$ rm file01.txt
rm: невозможно удалить 'file01.txt': Операция не позволена
guest2@earutynyan:/tmp$ su
Пароль:
root@earutynyan:/tmp# chmod -t /tmp
root@earutynyan:/tmp#
exit
guest2@earutynyan:/tmp$ cd /tmp
guest2@earutynyan:/tmp$ rm file01.txt
guest2@earutynyan:/tmp$
```

Рис. 4: исследование Sticky-бита

Выводы

Результаты выполнения лабораторной работы

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.