

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Солодовников Игорь НБИ-01-19

4 октября, 2022, 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.

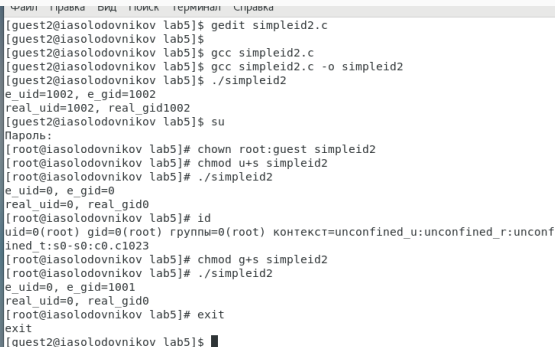
Выполнение лабораторной работы

Программа simpleid

```
[guest2@iasolodovnikov ~]$ cd lab5/
[guest2@iasolodovnikov lab5]$ touch simpleid.c
[guest2@iasolodovnikov lab5]$ touch simpleid2.c
[guest2@iasolodovnikov lab5]$ touch readfile.c
[guest2@iasolodovnikov lab5]$ gedit simpleid.c
[guest2@iasolodovnikov lab5]$
[guest2@iasolodovnikov lab5]$ gcc simpleid.c
[guest2@iasolodovnikov lab5]$ gcc simpleid.c -o simpleid
[guest2@iasolodovnikov lab5]$ ./simpleid
uid=1002, gid=1002
[guest2@iasolodovnikov lab5]$ id
uid=1002(guest2) gid=1002(guest2) rpyнны=1002(guest2),1001(guest),1004(guest3) к
онтекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@iasolodovnikov lab5]$
```

Figure 1: результат программы simpleid

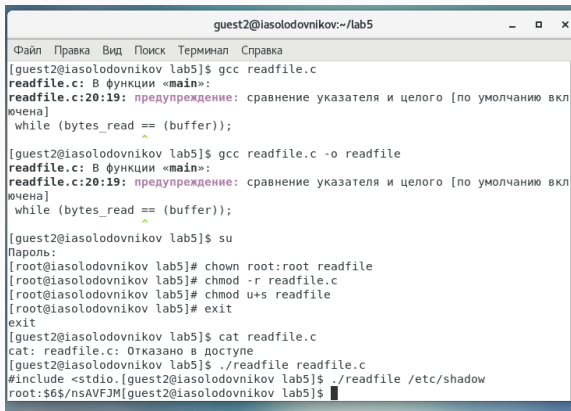
Программа simpleid2



```
Чтение Правка Вид Поиск Терминал Справка
[guest2@iasolodovnikov lab5]$ gedit simpleid2.c
[guest2@iasolodovnikov lab5]$
[guest2@iasolodovnikov lab5]$ gcc simpleid2.c
[guest2@iasolodovnikov lab5]$ gcc simpleid2.c -o simpleid2
[guest2@iasolodovnikov lab5]$ ./simpleid2
e_uid=1002, e_gid=1002
real_uid=1002, real_gid=1002
[guest2@iasolodovnikov lab5]$ su
Пароль:
[root@iasolodovnikov lab5]# chown root:guest simpleid2
[root@iasolodovnikov lab5]# chmod u+s simpleid2
[root@iasolodovnikov lab5]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@iasolodovnikov lab5]# id
uid=0(root) gid=0(root) rpnny=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@iasolodovnikov lab5]# chmod g+s simpleid2
[root@iasolodovnikov lab5]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@iasolodovnikov lab5]# exit
exit
[guest2@iasolodovnikov lab5]$
```

Figure 2: результат программы simpleid2

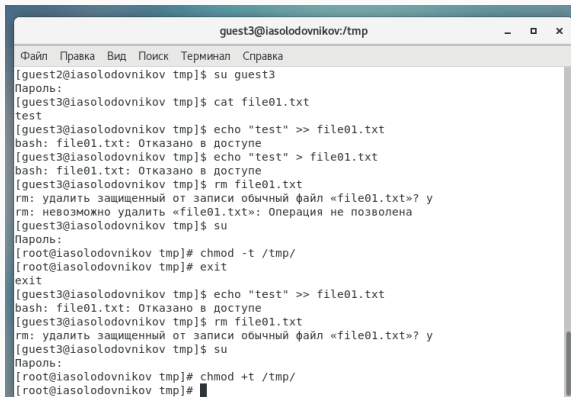
Программа readfile



```
guest2@iasolodovnikov:~/lab5
Файл Правка Вид Поиск Терминал Справка
[guest2@iasolodovnikov lab5]$ gcc readfile.c
readfile.c: В функции «main»:
readfile.c:20:19: предупреждение: сравнение указателя и целого [по умолчанию включена]
    while (bytes_read == (buffer));
                      ^
[guest2@iasolodovnikov lab5]$ gcc readfile.c -o readfile
readfile.c: В функции «main»:
readfile.c:20:19: предупреждение: сравнение указателя и целого [по умолчанию включена]
    while (bytes_read == (buffer));
                      ^
[guest2@iasolodovnikov lab5]$ su
Пароль:
[root@iasolodovnikov lab5]# chown root:root readfile
[root@iasolodovnikov lab5]# chmod -r readfile.c
[root@iasolodovnikov lab5]# chmod u+s readfile
[root@iasolodovnikov lab5]# exit
exit
[guest2@iasolodovnikov lab5]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest2@iasolodovnikov lab5]$ ./readfile readfile.c
#include <stdio.h>[guest2@iasolodovnikov lab5]$ ./readfile /etc/shadow
root:$6$nsAVFJM[guest2@iasolodovnikov lab5]$
```

Figure 3: результат программы readfile

Исследование Sticky-бита



```
guest3@iasolodovnikov:/tmp
Файл Правка Вид Поиск Терминал Справка
[guest2@iasolodovnikov tmp]$ su guest3
Пароль:
[guest3@iasolodovnikov tmp]$ cat file01.txt
test
[guest3@iasolodovnikov tmp]$ echo "test" >> file01.txt
bash: file01.txt: Отказано в доступе
[guest3@iasolodovnikov tmp]$ echo "test" > file01.txt
bash: file01.txt: Отказано в доступе
[guest3@iasolodovnikov tmp]$ rm file01.txt
rm: удалить защищенный от записи обычный файл «file01.txt»? y
rm: невозможно удалить «file01.txt»: Операция не позволена
[guest3@iasolodovnikov tmp]$ su
Пароль:
[root@iasolodovnikov tmp]# chmod -t /tmp/
[root@iasolodovnikov tmp]# exit
exit
[guest3@iasolodovnikov tmp]$ echo "test" >> file01.txt
bash: file01.txt: Отказано в доступе
[guest3@iasolodovnikov tmp]$ rm file01.txt
rm: удалить защищенный от записи обычный файл «file01.txt»? y
[guest3@iasolodovnikov tmp]$ su
Пароль:
[root@iasolodovnikov tmp]# chmod +t /tmp/
[root@iasolodovnikov tmp]#
```

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.