

Презентация по лабораторной работе № 5

Информационная безопасность

Кинсиклунон Доря Флора

06.10.2023

Российский университет дружбы народов, Москва, Россия

Информация

- Кинсиклунон Доря Флора
- студент группы НПМбд-02-20
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов

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.

Создание программы

Сначала созданы и выполнены две программы, имитирующие команду 'id', для отображения различных идентификаторов пользователя и группы. Затем, с правами суперпользователя, установлены биты SetUID и SetGID для этих программ. После этого, при выполнении программы, они получают соответствующие привилегии суперпользователя и группы. Это демонстрирует, как изменение битов SetUID и SetGID может повлиять на выполнение программ и их привилегии.



Рис. 1: simpleid.c



Рис. 2: Код

Создание программы(2)

Сначала создали программу для чтения файла (readfile.c) и скомпилировали её. Затем изменили права доступа к программе так, чтобы только пользователь root мог её читать, а гость - нет. Убедились, что гость не имеет доступа к файлу readfile.c через выполнение программы. Далее сменили владельца программы readfile и установили бит SetUID. После этого с помощью программы удалось прочитать файлы readfile.c и /etc/shadow. Этот процесс иллюстрирует изменение прав доступа и привилегий программы в системе.

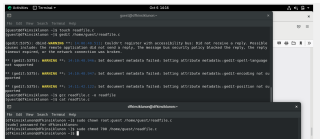


Рис. 3: readfile.c

```
...
#include <fcntl.h>
#include <unistd.h>
#include <stdio.h>
#include <sys/types.h>
#include <sys/stat.h>

int
main (int argc, char* argv[])
{
    unsigned char buffer[16];
    ssize_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;
}
```

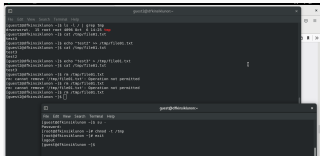
Рис. 4: Код

Исследование Sticky-бита

Сначала мы создали файл в каталоге /tmp, разрешив чтение и запись для всех пользователей. Затем, от имени пользователя guest2, мы попытались прочитать, дозаписать и переписать файл. Однако нам не удалось удалить файл.

Затем, суперпользователь снял Sticky-бит с каталога tmp и мы повторили действия с файлом. В этот раз удаление файла стало возможным.

Наконец, суперпользователь вернул Sticky-бит на каталог tmp, обеспечивая тем самым ограниченный доступ к файлам в этом каталоге, даже для суперпользователя. Эти действия демонстрируют влияние Sticky-бита на возможности удаления файлов в каталоге.



```
guest2@rocklinux:~$ cd /tmp
guest2@rocklinux:~/tmp$ touch test
guest2@rocklinux:~/tmp$ ls -l /tmp
drwxrwxrwt 12 root root 4096 Jul 8 14:25 tmp
-rw-rw-rw- 1 guest2 guest2 0 Jul 8 14:25 test
guest2@rocklinux:~/tmp$ rm test
rm: cannot remove 'test': Operation not permitted
guest2@rocklinux:~/tmp$ rm -f test
rm: cannot remove 'test': Operation not permitted
guest2@rocklinux:~/tmp$ rm -rf test
rm: cannot remove 'test': Operation not permitted
guest2@rocklinux:~/tmp$
```

```
root@rocklinux:~# cd /tmp
root@rocklinux:~/tmp$ touch test
root@rocklinux:~/tmp$ ls -l /tmp
drwxrwxrwt 12 root root 4096 Jul 8 14:25 tmp
-rw-rw-rw- 1 guest2 guest2 0 Jul 8 14:25 test
root@rocklinux:~/tmp$ rm test
rm: cannot remove 'test': Operation not permitted
root@rocklinux:~/tmp$ rm -f test
rm: cannot remove 'test': Operation not permitted
root@rocklinux:~/tmp$ rm -rf test
rm: cannot remove 'test': Operation not permitted
root@rocklinux:~/tmp$
```

Рис. 5: sticky-bit(1)



```
root@rocklinux:~# cd /tmp
root@rocklinux:~/tmp$ touch test
root@rocklinux:~/tmp$ ls -l /tmp
drwxrwxrwt 12 root root 4096 Jul 8 14:25 tmp
-rw-rw-rw- 1 guest2 guest2 0 Jul 8 14:25 test
root@rocklinux:~/tmp$ rm test
rm: cannot remove 'test': Operation not permitted
root@rocklinux:~/tmp$ rm -f test
rm: cannot remove 'test': Operation not permitted
root@rocklinux:~/tmp$ rm -rf test
rm: cannot remove 'test': Operation not permitted
root@rocklinux:~/tmp$
```

```
root@rocklinux:~# cd /tmp
root@rocklinux:~/tmp$ touch test
root@rocklinux:~/tmp$ ls -l /tmp
drwxrwxrwt 12 root root 4096 Jul 8 14:25 tmp
-rw-rw-rw- 1 guest2 guest2 0 Jul 8 14:25 test
root@rocklinux:~/tmp$ rm test
rm: cannot remove 'test': Operation not permitted
root@rocklinux:~/tmp$ rm -f test
rm: cannot remove 'test': Operation not permitted
root@rocklinux:~/tmp$ rm -rf test
rm: cannot remove 'test': Operation not permitted
root@rocklinux:~/tmp$
```

Рис. 6: sticky-bit(2)

Вывод

В ходе выполнения данной лабораторной работы я изучила механизмы изменения идентификаторов, применение 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.