

Лабораторная работа № 5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Абдуллаев Сайидазизхон Шухратович

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.

Ход работы

Написание, запуск и результат работы первой программы

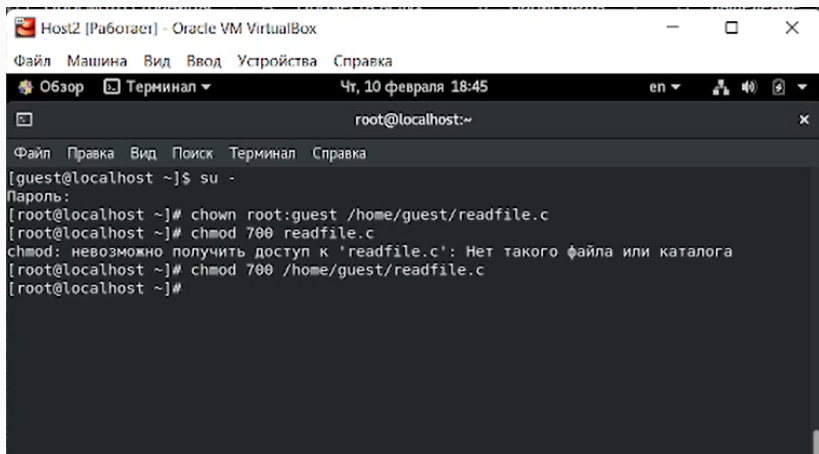
```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@localhost ~]$ nano simpleid.c  
[guest@localhost ~]$ ls -l  
итого 4  
drwx----- 2 guest guest 19 фев 10 17:44 dir1  
-rw-rw-r-- 1 guest guest 172 фев 10 18:20 simpleid.c  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 Видео  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 Документы  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 Загрузки  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 Изображения  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 Музыка  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 Общедоступные  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 'Рабочий стол'  
drwxr-xr-x 2 guest guest 6 фев 9 15:39 Шаблоны  
[guest@localhost ~]$ gcc simpleid.c -o simpleid  
[guest@localhost ~]$ ./simpleid  
uid=1001, gid=1001  
[guest@localhost ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@localhost ~]$
```

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

Смена владельца и установление SetUID-бита на программу simpleid2

```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@localhost ~]$ su -  
Пароль:  
[root@localhost ~]# chown root:guest /home/guest/simpleid2  
[root@localhost ~]# chmod u+s /home/guest/simpleid2  
[root@localhost ~]# ls -l simpleid2  
ls: невозможно получить доступ к 'simpleid2': Нет такого файла или каталога  
[root@localhost ~]# exit  
выход  
[guest@localhost ~]$ ls -l simpleid2  
-rwsrwxr-x. 1 root guest 18152 фев 10 18:27 simpleid2  
[guest@localhost ~]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@localhost ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@localhost ~]$
```

Установка прав и владельца на программе readfile и файле readfile.c



The screenshot shows a terminal window titled "Host2 [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar is a toolbar with icons for "Обзор", "Терминал", and a clock showing "Чт, 10 февраля 18:45". The terminal itself has a title bar "root@localhost:~" and a menu bar with "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The terminal content shows the following commands and output:

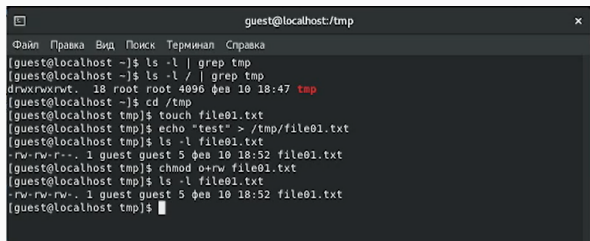
```
[guest@localhost ~]$ su -  
Пароль:  
[root@localhost ~]# chown root:guest /home/guest/readfile.c  
[root@localhost ~]# chmod 700 readfile.c  
chmod: невозможно получить доступ к 'readfile.c': Нет такого файла или каталога  
[root@localhost ~]# chmod 700 /home/guest/readfile.c  
[root@localhost ~]#
```

```
[guest@localhost ~]$ ./readfile readfile.c
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>

int main(int argc, char* argv[]){
    unsigned char buffer[16];
    size_t bytes_read;
    int i;

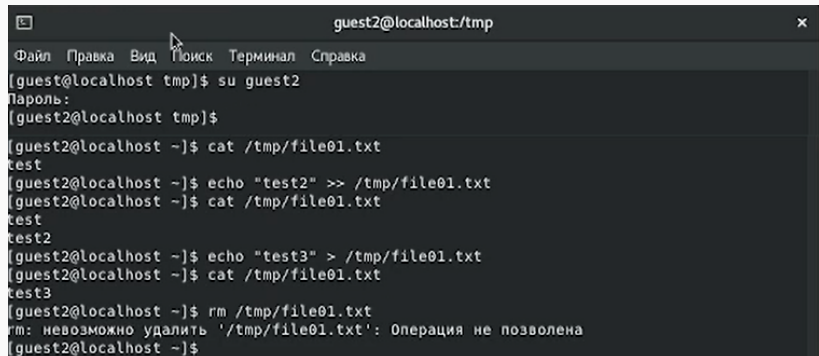
    int fd = open (argv[1], O_RDONLY);
    do{
        bytes_read = read (fd, buffer, sizeof(buffer));
        for(i = 0; i<bytes_read; ++i)
            printf("%c", buffer[i]);
    }
    while (bytes_read == sizeof(buffer));
    close (fd);
return 0;
}
[guest@localhost ~]$ ./readfile /etc/shadow
```


Проверка файла в директории со Sticky-битом



```
guest@localhost:/tmp
Файл  Правка  Вид  Поиск  Терминал  Справка
(guest@localhost ~)$ ls -l | grep tmp
(guest@localhost ~)$ ls -l / | grep tmp
drwxrwxrwt. 18 root root 4096 фев 10 18:47 tmp
(guest@localhost ~)$ cd /tmp
(guest@localhost tmp)$ touch file01.txt
(guest@localhost tmp)$ echo "test" > /tmp/file01.txt
(guest@localhost tmp)$ ls -l file01.txt
-rw-rw-r--. 1 guest guest 5 фев 10 18:52 file01.txt
(guest@localhost tmp)$ chmod o+rw file01.txt
(guest@localhost tmp)$ ls -l file01.txt
-rw-rw-rw-. 1 guest guest 5 фев 10 18:52 file01.txt
(guest@localhost tmp)$
```

Проверка файла в директории без Sticky-бита



```
guest2@localhost:/tmp
Файл  Правка  Вид  Поиск  Терминал  Справка
(guest@localhost tmp)$ su guest2
Пароль:
(guest2@localhost tmp)$
(guest2@localhost ~)$ cat /tmp/file01.txt
test
(guest2@localhost ~)$ echo "test2" >> /tmp/file01.txt
(guest2@localhost ~)$ cat /tmp/file01.txt
test
test2
(guest2@localhost ~)$ echo "test3" > /tmp/file01.txt
(guest2@localhost ~)$ cat /tmp/file01.txt
test3
(guest2@localhost ~)$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
(guest2@localhost ~)$
```

- В результате выполнения данной работы были изучены механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Кроме того, получены практические навыки работы в консоли с дополнительными атрибутами, рассмотрена работа механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.