

Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Старовойтов Е. С.

1 октября 2024

Цель 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.

Задание

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Выполнение лабораторной работы

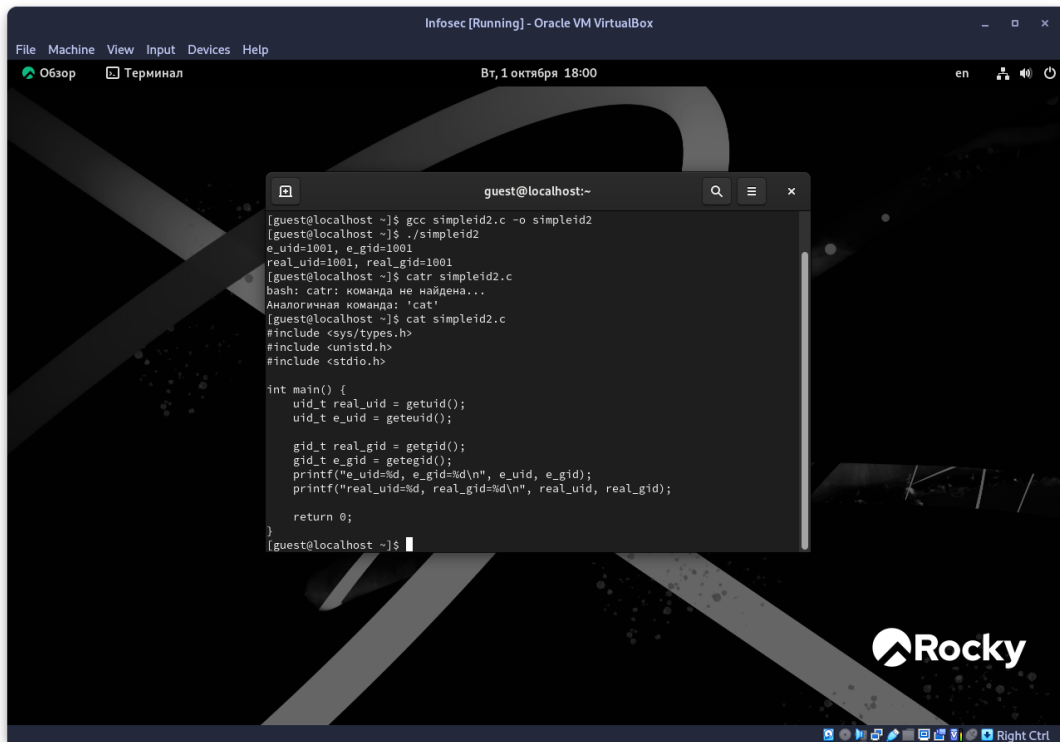
Шаги 1-5

```
Infosec [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Обзор Терминал Вт, 1 октября 17:56 en

guest@localhost:~
[guest@localhost ~]$ vim simpleid.c
[guest@localhost ~]$ gcc simpleid.c -o simpleid
[guest@localhost ~]$ ls
simpleid  simpleid.c
[guest@localhost ~]$ ./simpleid
uid=1001, gid=1001
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) rгруппы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost ~]$ cat simpleid.c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int main() {
    uid_t uid = geteuid();
    gid_t gid = getegid();
    printf("uid=%d, gid=%d\n", uid, gid);
    return 0;
}
[guest@localhost ~]$
```

Шаги 6-7



The screenshot shows a virtual machine window titled "Infosec [Running] - Oracle VM VirtualBox". The desktop background is the Rocky Linux logo. A terminal window is open, displaying the following commands and output:

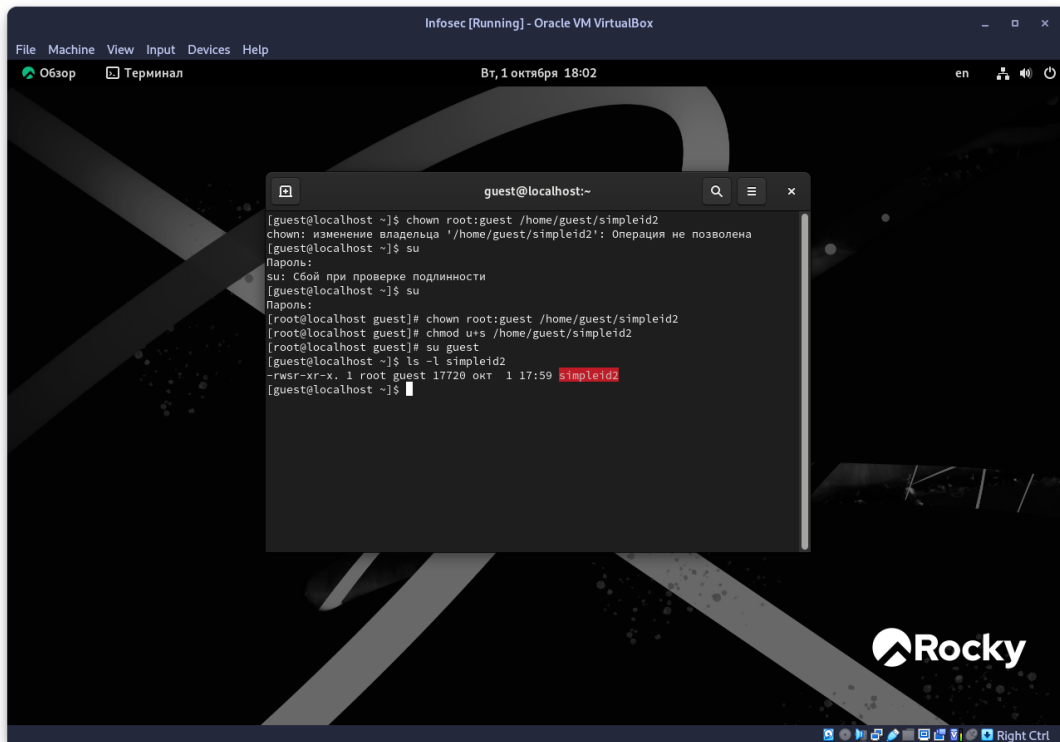
```
guest@localhost:~$ gcc simpleid2.c -o simpleid2
guest@localhost:~$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
guest@localhost:~$ catr simpleid2.c
bash: catr: команда не найдена...
Аналогичная команда: 'cat'
guest@localhost:~$ cat simpleid2.c
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int main() {
    uid_t real_uid = getuid();
    uid_t e_uid = geteuid();

    gid_t real_gid = getgid();
    gid_t e_gid = getegid();
    printf("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
    printf("real_uid=%d, real_gid=%d\n", real_uid, real_gid);

    return 0;
}
guest@localhost:~$
```

Шаги 8-10

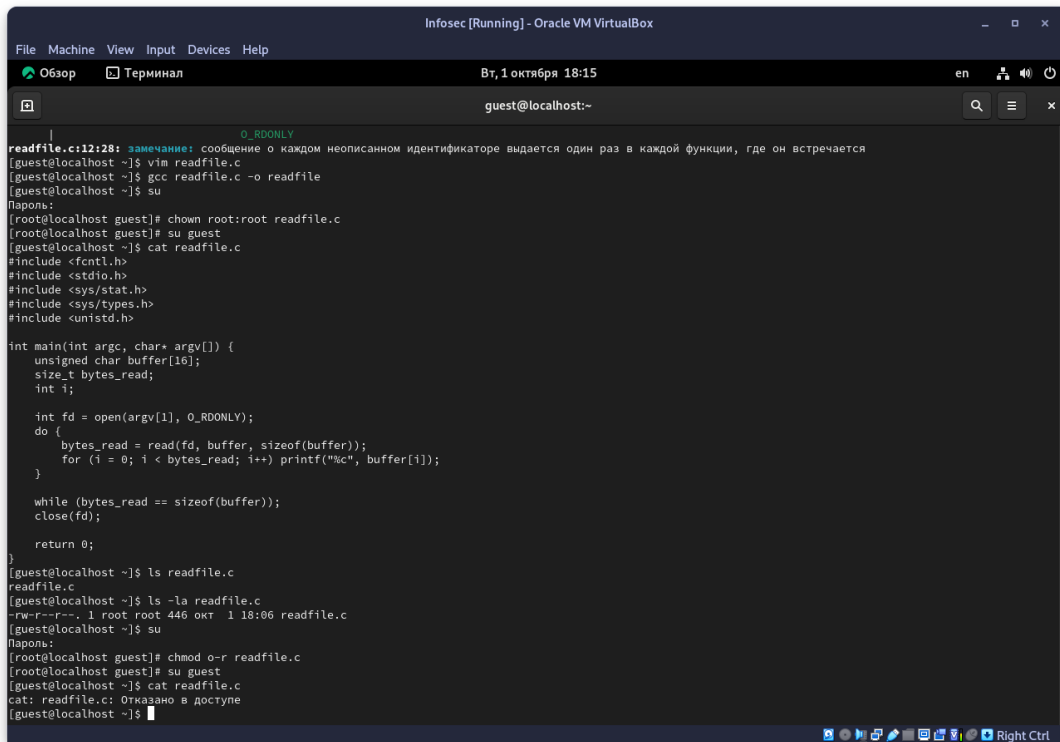


The screenshot shows a terminal window titled "Infosec [Running] - Oracle VM VirtualBox" with a menu bar (File, Machine, View, Input, Devices, Help) and a status bar (Вт, 1 октября 18:02, en, volume, power). The terminal content is as follows:

```
guest@localhost:~  
[guest@localhost ~]$ chown root:guest /home/guest/simpleid2  
chown: изменение владельца '/home/guest/simpleid2': Операция не позволена  
[guest@localhost ~]$ su  
Пароль:  
su: Сбой при проверке подлинности  
[guest@localhost ~]$ su  
Пароль:  
[root@localhost guest]# chown root:guest /home/guest/simpleid2  
[root@localhost guest]# chmod u+s /home/guest/simpleid2  
[root@localhost guest]# su guest  
[guest@localhost ~]$ ls -l simpleid2  
-rwsr-xr-x. 1 root guest 17720 окт  1 17:59 simpleid2  
[guest@localhost ~]$
```

The background of the VM desktop features a dark theme with a large stylized 'X' and the Rocky Linux logo in the bottom right corner. The system tray at the bottom includes icons for network, volume, and power, along with the text "Right Ctrl".

Шаги 11-17



```
Infosec [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Обзор Терминал Вт, 1 октября 18:15 en
guest@localhost:~

readfile.c:12:28: замечание: сообщение о каждом неопisanном идентификаторе выдается один раз в каждой функции, где он встречается
                          O_RDONLY
[guest@localhost ~]$ vim readfile.c
[guest@localhost ~]$ gcc readfile.c -o readfile
[guest@localhost ~]$ su
Пароль:
[root@localhost guest]# chown root:root readfile.c
[root@localhost guest]# su guest
[guest@localhost ~]$ cat readfile.c
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>

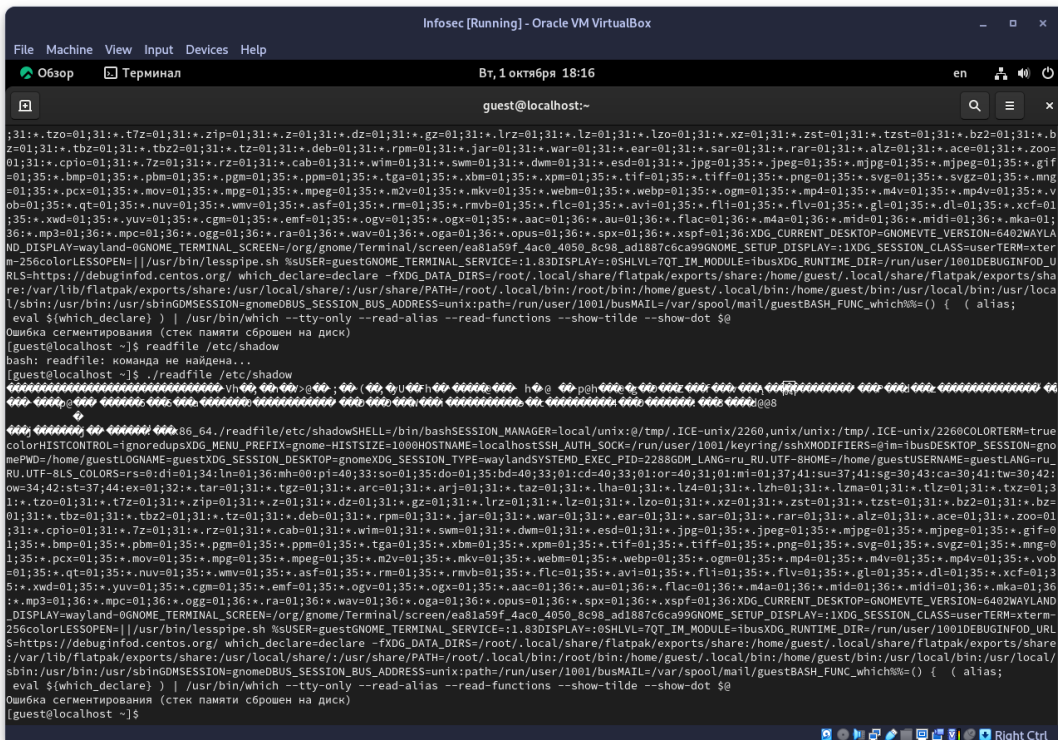
int main(int argc, char* argv[]) {
    unsigned char buffer[16];
    size_t bytes_read;
    int i;

    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]);
    }

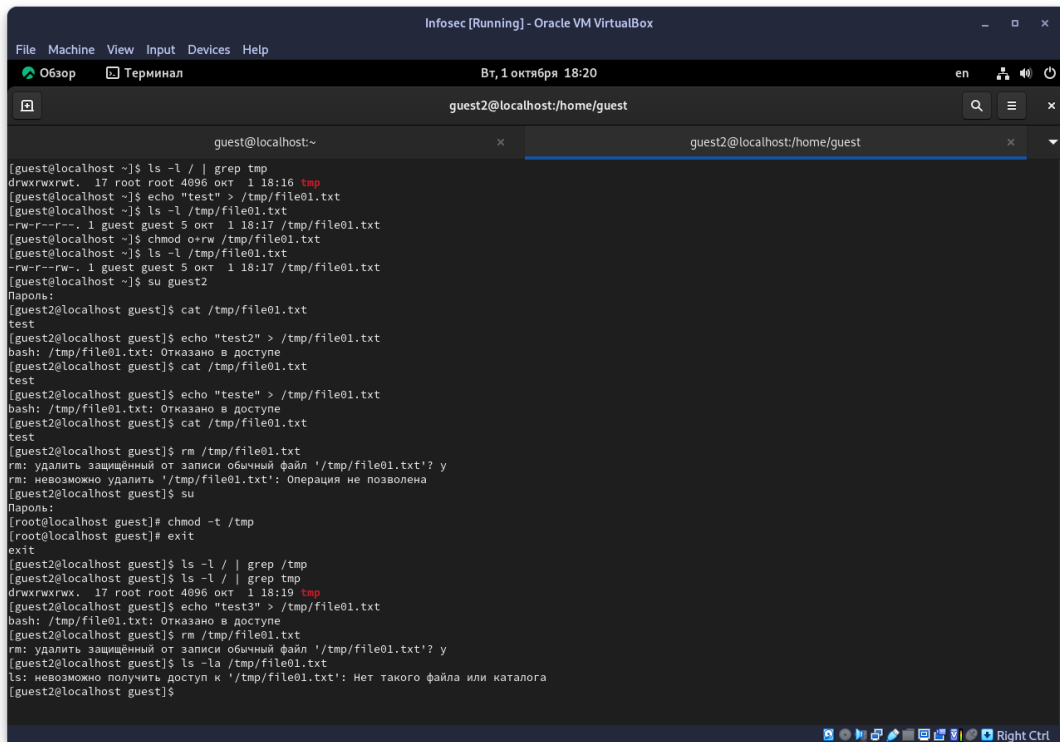
    while (bytes_read == sizeof(buffer));
    close(fd);

    return 0;
}
[guest@localhost ~]$ ls readfile.c
readfile.c
[guest@localhost ~]$ ls -la readfile.c
-rw-r--r-- 1 root root 446 окт 18:06 readfile.c
[guest@localhost ~]$ su
Пароль:
[root@localhost guest]# chmod o-r readfile.c
[root@localhost guest]# su guest
[guest@localhost ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@localhost ~]$
```

Шага 18-19



Исследование sticky-бита



```
Infosec [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Обзор Терминал
Вт, 1 октября 18:20
en
guest2@localhost/home/guest

guest@localhost~
[guest@localhost ~]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 окт 1 18:16 tmp
[guest@localhost ~]$ echo "test" > /tmp/file01.txt
[guest@localhost ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 окт 1 18:17 /tmp/file01.txt
[guest@localhost ~]$ chmod o+rw /tmp/file01.txt
[guest@localhost ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 окт 1 18:17 /tmp/file01.txt
[guest@localhost ~]$ su guest2
Пароль:
[guest2@localhost guest]$ cat /tmp/file01.txt
test
[guest2@localhost guest]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@localhost guest]$ cat /tmp/file01.txt
test
[guest2@localhost guest]$ echo "teste" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@localhost guest]$ cat /tmp/file01.txt
test
[guest2@localhost guest]$ rm /tmp/file01.txt
rm: удалить защищенный от записи обычный файл '/tmp/file01.txt'? y
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest2@localhost guest]$ su
Пароль:
[root@localhost guest]# chmod -t /tmp
[root@localhost guest]# exit
exit
[guest2@localhost guest]$ ls -l / | grep /tmp
[guest2@localhost guest]$ ls -l / | grep tmp
drwxrwxrwx. 17 root root 4096 окт 1 18:19 tmp
[guest2@localhost guest]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@localhost guest]$ rm /tmp/file01.txt
rm: удалить защищенный от записи обычный файл '/tmp/file01.txt'? y
[guest2@localhost guest]$ ls -la /tmp/file01.txt
ls: невозможно получить доступ к '/tmp/file01.txt': Нет такого файла или каталога
[guest2@localhost guest]$
```

Выводы

Я получил практические навыки работы в консоли с расширенными атрибутами файлов.