

Лабораторная работа №5

Информационная безопасность

Леонтьева К. А., НПМбд-01-19

25 сентября 2022

Российский университет дружбы народов

Москва, Россия

- 1) Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов

- 1) Создать и выполнить программу, выводящую uid и gid, сравнить вывод до и после добавления SetUID и SetGID
- 2) Создать программу для чтения файлов, проверить возможность чтения до и после добавления SetUID
- 3) Исследовать Sticky-бит при записи и удалении файла в папке /tmp

Ход выполнения лабораторной работы

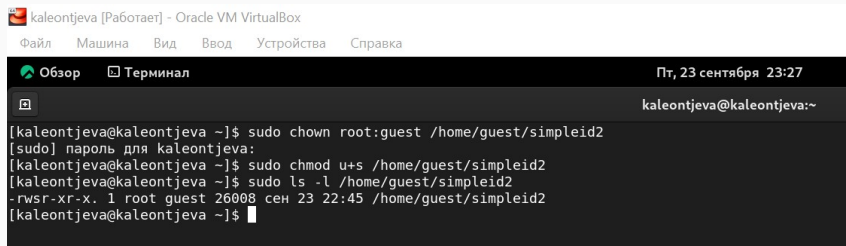
- Создала программу simpleid2, выводящую uid и gid. Сравнила ее вывод с командой id - если дополнительные биты не установлены, то вывод совпадает

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

```
1#include <sys/types.h>
2#include <unistd.h>
3#include <stdio.h>
4
5int
6main ()
7{
8    uid_t real_uid = getuid ();
9    uid_t e_uid = geteuid ();
10
11    gid_t real_gid = getgid ();
12    gid_t e_gid = getegid ();
13
14    printf("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
15    printf("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
16
17    return 0;
18}
```

Figure 1: Рис.1: Вывод программы simpleid2

- Сменила пользователя файла на root и установила SetUID-бит

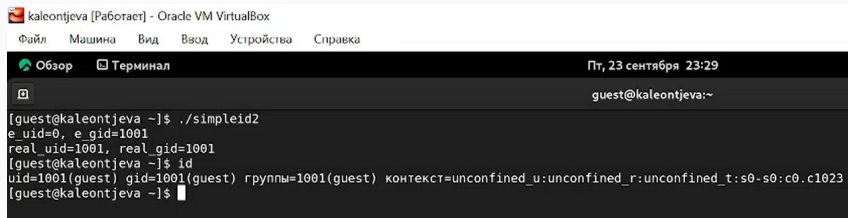


The screenshot shows a terminal window titled "kaleontjeva [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar, there are tabs for "Обзор" and "Терминал", and a clock showing "Пт, 23 сентября 23:27". The terminal prompt is "kaleontjeva@kaleontjeva:~". The following commands and their outputs are shown:

```
[kaleontjeva@kaleontjeva ~]$ sudo chown root:guest /home/guest/simpleid2
[sudo] пароль для kaleontjeva:
[kaleontjeva@kaleontjeva ~]$ sudo chmod u+s /home/guest/simpleid2
[kaleontjeva@kaleontjeva ~]$ sudo ls -l /home/guest/simpleid2
-rwsr-xr-x. 1 root guest 26008 сен 23 22:45 /home/guest/simpleid2
[kaleontjeva@kaleontjeva ~]$
```

Figure 2: Рис.2: Смена пользователя и установка SetUID

- Запустила программы `simpleid2` и `id`. Теперь появились различия в `uid`

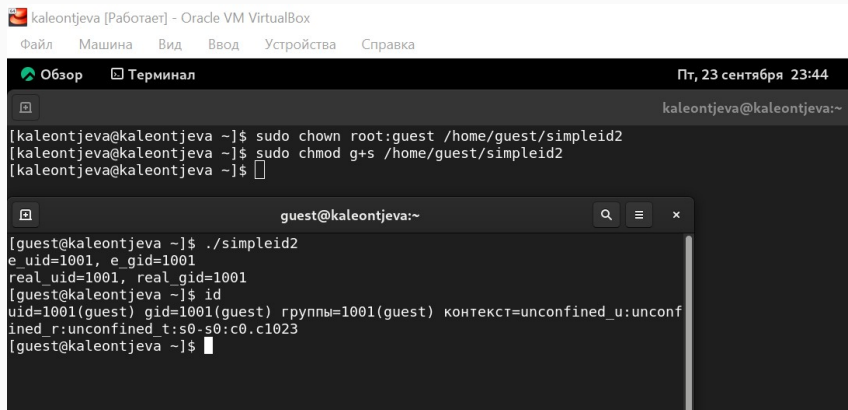


The screenshot shows a terminal window titled "kaleontjeva [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar are two tabs: "Обзор" and "Терминал". The terminal output is as follows:

```
[guest@kaleontjeva ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@kaleontjeva ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@kaleontjeva ~]$
```

Figure 3: Рис.3: Вывод программы `simpleid2` после установки `SetUID`

- Аналогично установила SetGID-бит. Получила различия с предыдущим пунктом



The screenshot shows a terminal window titled "kaleontjeva [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar, there are tabs for "Обзор" and "Терминал". The terminal shows the following commands and output:

```
[kaleontjeva@kaleontjeva ~]$ sudo chown root:guest /home/guest/simpleid2
[kaleontjeva@kaleontjeva ~]$ sudo chmod g+s /home/guest/simpleid2
[kaleontjeva@kaleontjeva ~]$
```

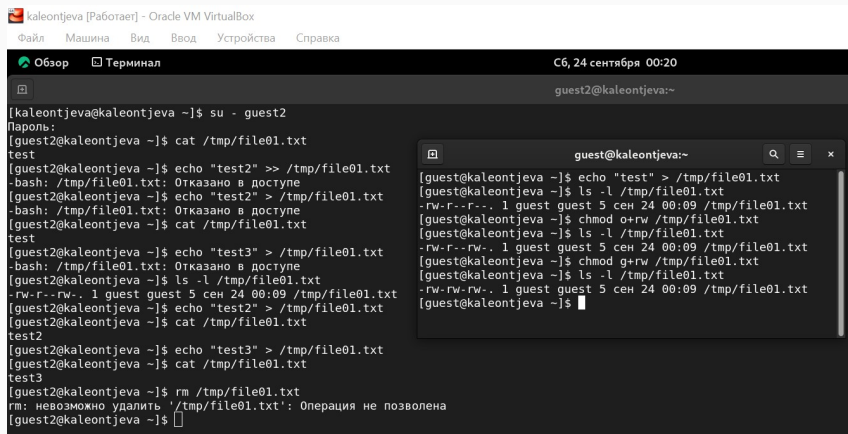
Below this, there is a sub-terminal window titled "guest@kaleontjeva:~". It shows the execution of the program and the output of the 'id' command:

```
[guest@kaleontjeva ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@kaleontjeva ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@kaleontjeva ~]$
```

Figure 4: Рис.4: Вывод программы simpleid2 после установки SetGID

Ход выполнения лабораторной работы

- Попробовала прочитать, дозаписать и перезаписать текст в файле file01.txt - операции выполнились без ошибок. Удалить файл не удалось.



The screenshot shows a terminal window titled "kaleontjeva [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar are two tabs: "Обзор" and "Терминал". The terminal output shows the following commands and results:

```
[kaleontjeva@kaleontjeva ~]$ su - guest2
Пароль:
[guest2@kaleontjeva ~]$ cat /tmp/file01.txt
test
[guest2@kaleontjeva ~]$ echo "test2" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Отказано в доступе
[guest2@kaleontjeva ~]$ echo "test2" > /tmp/file01.txt
-bash: /tmp/file01.txt: Отказано в доступе
[guest2@kaleontjeva ~]$ cat /tmp/file01.txt
test
[guest2@kaleontjeva ~]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Отказано в доступе
[guest2@kaleontjeva ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 сен 24 00:09 /tmp/file01.txt
[guest2@kaleontjeva ~]$ echo "test2" > /tmp/file01.txt
[guest2@kaleontjeva ~]$ cat /tmp/file01.txt
test2
[guest2@kaleontjeva ~]$ echo "test3" > /tmp/file01.txt
[guest2@kaleontjeva ~]$ cat /tmp/file01.txt
test3
[guest2@kaleontjeva ~]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest2@kaleontjeva ~]$
```

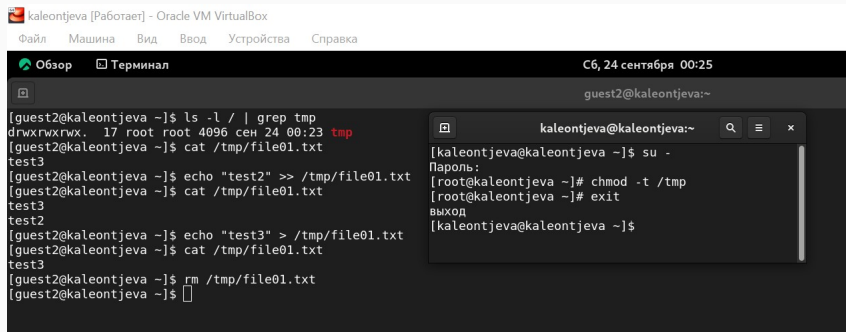
On the right side of the terminal window, there is a smaller, semi-transparent terminal window titled "guest@kaleontjeva:~". It shows the following commands and results:

```
[guest@kaleontjeva ~]$ echo "test" > /tmp/file01.txt
[guest@kaleontjeva ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 сен 24 00:09 /tmp/file01.txt
[guest@kaleontjeva ~]$ chmod o+rw /tmp/file01.txt
[guest@kaleontjeva ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 сен 24 00:09 /tmp/file01.txt
[guest@kaleontjeva ~]$ chmod g+rw /tmp/file01.txt
[guest@kaleontjeva ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 сен 24 00:09 /tmp/file01.txt
[guest@kaleontjeva ~]$
```

Figure 5: Рис.5: Действия над файлом file01.txt при наличии Sticky-бита

Ход выполнения лабораторной работы

- После удаления Sticky-бита от имени суперпользователя удаление файла file01.txt стало возможным от имени пользователя, не являющегося его владельцем



The screenshot shows a terminal window titled "kaleontjeva [Работает] - Oracle VM VirtualBox". The terminal output shows the following commands and results:

```
[guest2@kaleontjeva ~]$ ls -l / | grep tmp
drwxrwxrwx. 17 root root 4096 сен 24 00:23 tmp
[guest2@kaleontjeva ~]$ cat /tmp/file01.txt
test3
[guest2@kaleontjeva ~]$ echo "test2" >> /tmp/file01.txt
[guest2@kaleontjeva ~]$ cat /tmp/file01.txt
test3
test2
[guest2@kaleontjeva ~]$ echo "test3" > /tmp/file01.txt
[guest2@kaleontjeva ~]$ cat /tmp/file01.txt
test3
[guest2@kaleontjeva ~]$ rm /tmp/file01.txt
[guest2@kaleontjeva ~]$
```

An inset window shows the command sequence to remove the sticky bit:

```
kaleontjeva@kaleontjeva:~$ su -
Пароль:
[root@kaleontjeva ~]# chmod -t /tmp
[root@kaleontjeva ~]# exit
выход
[kaleontjeva@kaleontjeva ~]$
```

Figure 6: Рис.6: Действия над файлом file01.txt после удаления Sticky-бита

- В ходе выполнения данной лабораторной работы я изучила механизмы изменения идентификаторов, применение SetUID- и Sticky-битов. Рассмотрела работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.