

# РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

## ОТЧЕТ

### ПО ЛАБОРАТОРНОЙ РАБОТЕ № 5

Дисциплина: Основы информационной безопасности

Название работы: Дискреционное разграничение прав в Linux.

Исследование влияния дополнительных атрибутов

Студент: Теплякова Анастасия

Группа: НПМбд-02-17

МОСКВА

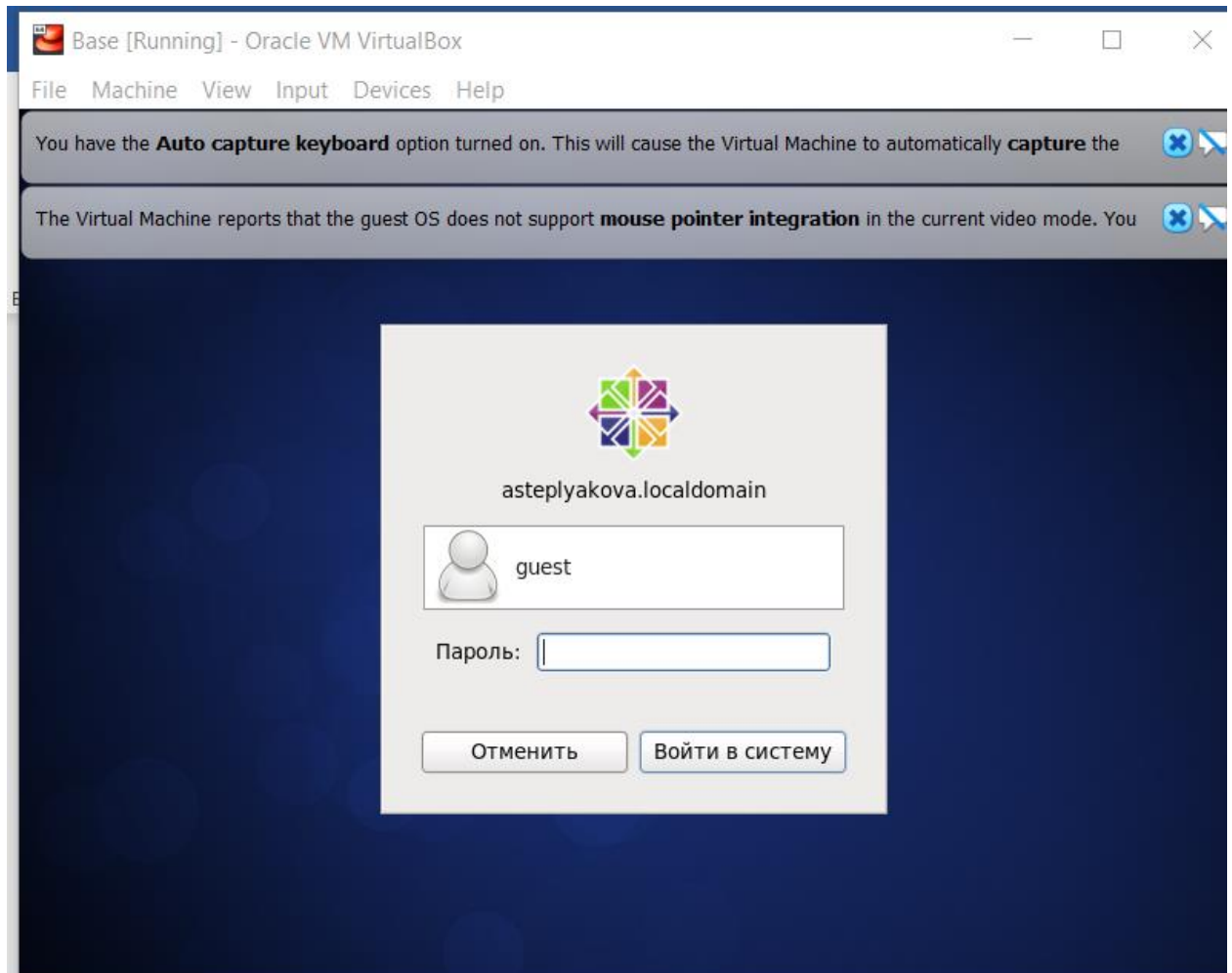
2022 г.

## Цель работы

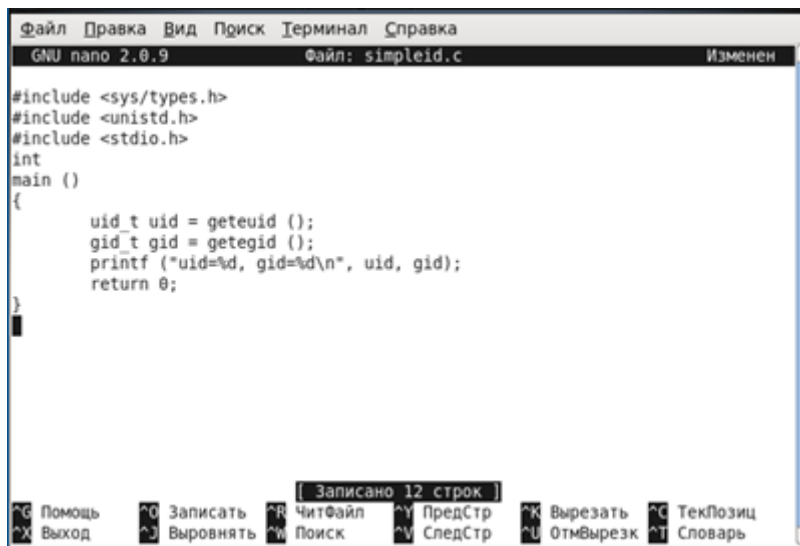
Изучение механизмов изменения идентификаторов, применения SetUID и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

## Выполнение работы

1. Вошла в систему от имени пользователя guest.



2. Создала программу simpleid.c.



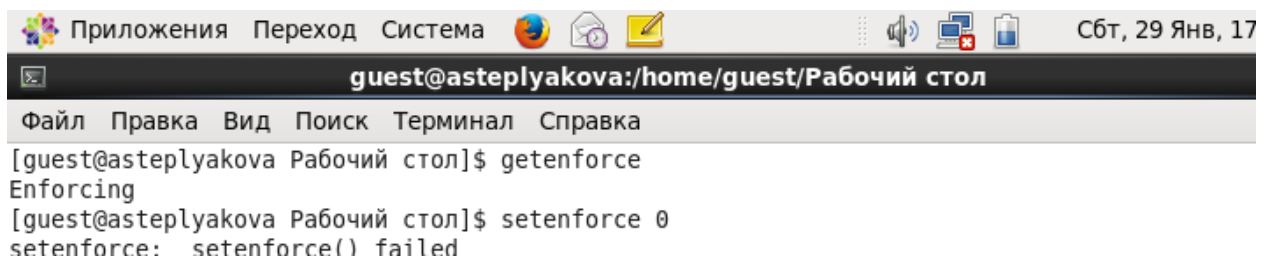
```
Файл Правка Вид Поиск Терминал Справка
GNU nano 2.0.9 Файл: simpleid.c Изменен

#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;
}

[ Записано 12 строк ]
Помощь Записать ЧитФайл ПредСтр Вырезать ТекЛозиц
Выход Вывернуть Поиск СледСтр ОтмВырезк Словарь
```

3. Скомпилировала программу и убедилась, что файл программы создан: `gcc simpleid.c -o simpleid`

4. Выполнила программу simpleid: `./simpleid`

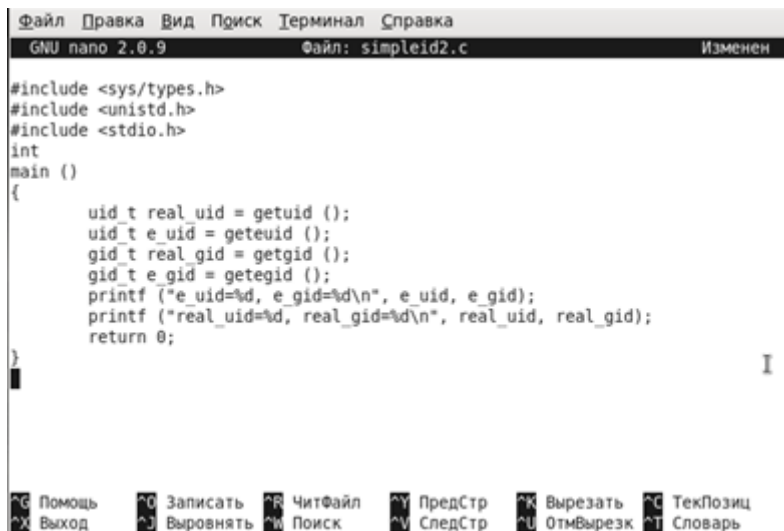


```
Приложения Переход Система Сбт, 29 Янв, 17
guest@asteplyakova:/home/guest/Рабочий стол
Файл Правка Вид Поиск Терминал Справка
[guest@asteplyakova Рабочий стол]$ getenforce
Enforcing
[guest@asteplyakova Рабочий стол]$ setenforce 0
setenforce: setenforce() failed
```

5. Выполнила системную программу `id` и сравнил полученный результат с данными предыдущего пункта задания: программа работает верно, результаты совпадают.

```
[guest@asteplyakova Рабочий стол]$ whereis gcc
gcc:
[guest@asteplyakova Рабочий стол]$ whereis g++
g++:
[guest@asteplyakova Рабочий стол]$ gcc simpleid.c -o simpleid
bash: gcc: команда не найдена
[guest@asteplyakova Рабочий стол]$ gcc -c file.c
bash: gcc: команда не найдена
[guest@asteplyakova Рабочий стол]$ yum install gcc
Загружены модули: fastestmirror, refresh-packagekit, security
Необходимы привилегии суперпользователя для выполнения этой команды.
```

6. Усложнила программу, добавив вывод действительных идентификаторов:



```
Файл Правка Вид Поиск Терминал Справка
GNU nano 2.0.9 Файл: simpleid2.c Изменен

#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;
}
```

Получившуюся программу назвал simpleid2.c

7. Скомпилировала и запустила simpleid2.c

8. От имени суперпользователя выполнил команды:

```
chown root:guest /home/guest/simpleid2
```

```
chmod u+s /home/guest/simpleid2
```

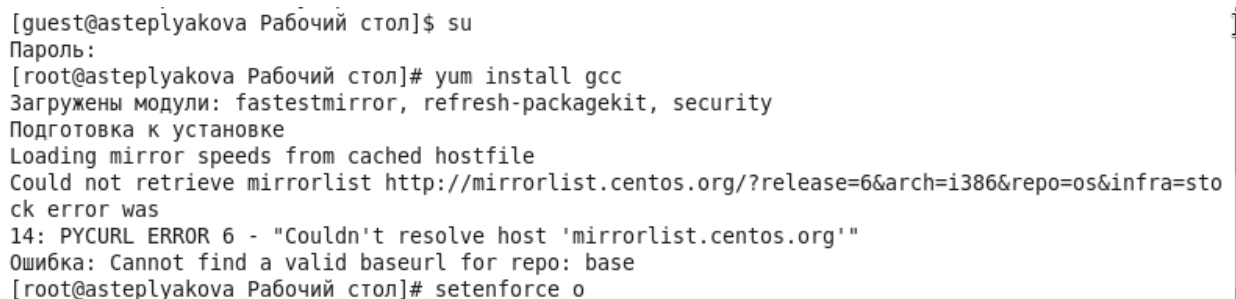
С помощью этих команд файлу simpleid2 изменил владельца и группу на root и guest соответственно, а также установил на файл SetUID-бит.

9. Временно повысила свои права с помощью команды *su*

```
[guest@asteplyakova Рабочий стол]$ whereis gcc
gcc:
[guest@asteplyakova Рабочий стол]$ whereis g++
g++:
[guest@asteplyakova Рабочий стол]$ gcc simpleid.c -o simpleid
bash: gcc: команда не найдена
[guest@asteplyakova Рабочий стол]$ gcc -c file.c
bash: gcc: команда не найдена
[guest@asteplyakova Рабочий стол]$ yum install gcc
Загружены модули: fastestmirror, refresh-packagekit, security
Необходимы привилегии суперпользователя для выполнения этой команды.
```

10. Выполнила проверку правильности установки новых атрибутов и смены владельца файла simpleid2: *ls -l simpleid2*

11. Запустила simpleid2 и *id*:

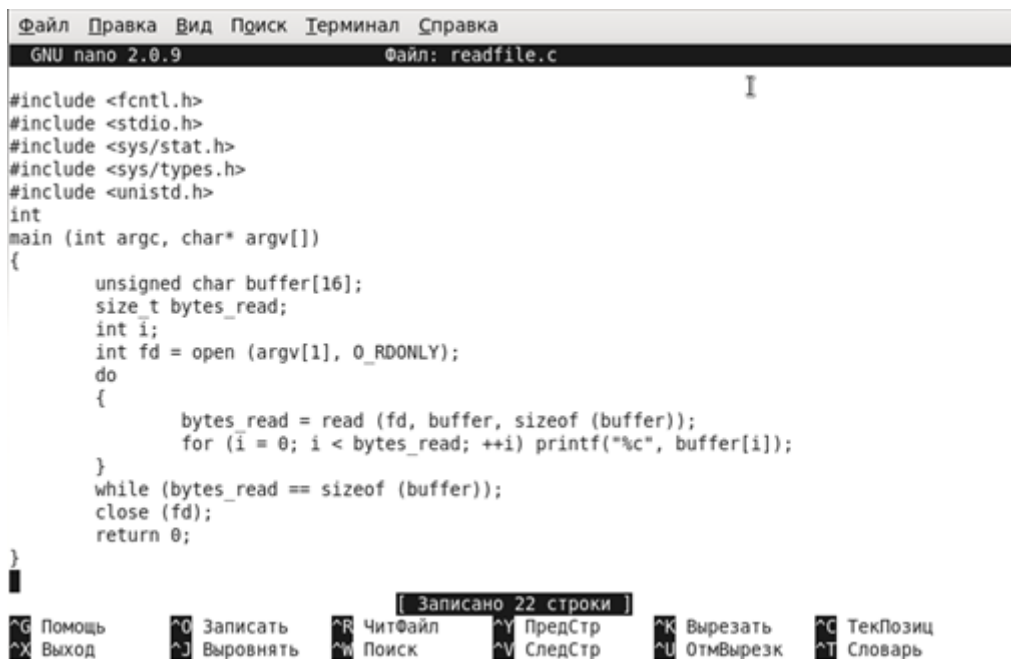


```
[guest@asteplyakova Рабочий стол]$ su
Пароль:
[root@asteplyakova Рабочий стол]# yum install gcc
Загружены модули: fastestmirror, refresh-packagekit, security
Подготовка к установке
Loading mirror speeds from cached hostfile
Could not retrieve mirrorlist http://mirrorlist.centos.org/?release=6&arch=i386&repo=os&infra=stock
error was
14: PYCURL ERROR 6 - "Couldn't resolve host 'mirrorlist.centos.org'"
Ошибка: Cannot find a valid baseurl for repo: base
[root@asteplyakova Рабочий стол]# setenforce 0
```

Результаты совпадают.

12. Прodelала тоже самое относительно SetGID-бита.

13. Создала программу readfile.c



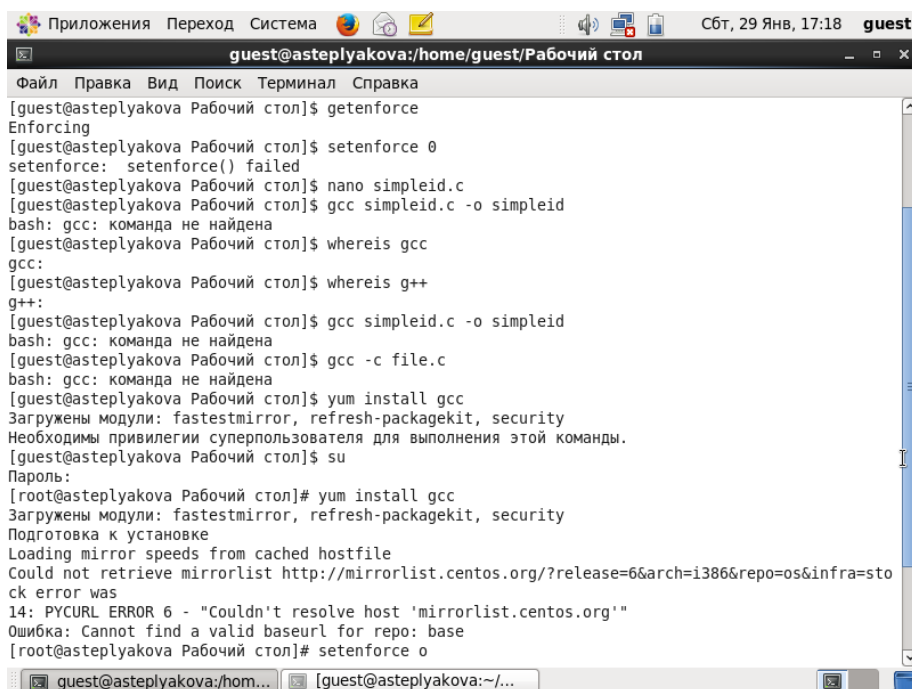
```
Файл  Правка  Вид  Поиск  Терминал  Справка
GNU nano 2.0.9      Файл: readfile.c

#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;
}

[ Записано 22 строки ]
^G Помощь  ^O Записать  ^R ЧитФайл  ^Y ПредСтр  ^K Вырезать  ^C ТекПозиц
^X Выход    ^J Вывернуть ^W Поиск    ^V СледСтр  ^U ОтмВырезк ^T Словарь
```

14. Откомпилировала её.

15. Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог.



```
Приложения  Переход  Система
guest@asteptyakova:/home/guest/Рабочий стол
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@asteptyakova Рабочий стол]$ getenforce
Enforcing
[guest@asteptyakova Рабочий стол]$ setenforce 0
setenforce: setenforce() failed
[guest@asteptyakova Рабочий стол]$ nano simpleid.c
[guest@asteptyakova Рабочий стол]$ gcc simpleid.c -o simpleid
bash: gcc: команда не найдена
[guest@asteptyakova Рабочий стол]$ whereis gcc
gcc:
[guest@asteptyakova Рабочий стол]$ whereis g++
g++:
[guest@asteptyakova Рабочий стол]$ gcc simpleid.c -o simpleid
bash: gcc: команда не найдена
[guest@asteptyakova Рабочий стол]$ gcc -c file.c
bash: gcc: команда не найдена
[guest@asteptyakova Рабочий стол]$ yum install gcc
Загружены модули: fastestmirror, refresh-packagekit, security
Необходимы привилегии суперпользователя для выполнения этой команды.
[guest@asteptyakova Рабочий стол]$ su
Пароль:
[root@asteptyakova Рабочий стол]# yum install gcc
Загружены модули: fastestmirror, refresh-packagekit, security
Подготовка к установке
Loading mirror speeds from cached hostfile
Could not retrieve mirrorlist http://mirrorlist.centos.org/?release=6&arch=i386&repo=os&infra=sto
ck error was
14: PYCURL ERROR 6 - "Couldn't resolve host 'mirrorlist.centos.org'"
Ошибка: Cannot find a valid baseurl for repo: base
[root@asteptyakova Рабочий стол]# setenforce 0
```

16. Проверила, что пользователь guest не может прочитать файл readfile.c.

17. Сменила у программы readfile владельца и установила SetU'D-бит.

18. Проверила, может ли программа readfile прочитать файл readfile.c

19. Проверила, может ли программа readfile прочитать файл /etc/shadow. Может.

## Вывод:

Благодаря данной лабораторной работе, я изучила механизмы изменения идентификаторов, применения SetUID-. 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.