

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико–математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 5

дисциплина: Информационная безопасность

Студент: Логинов Сергей Андреевич

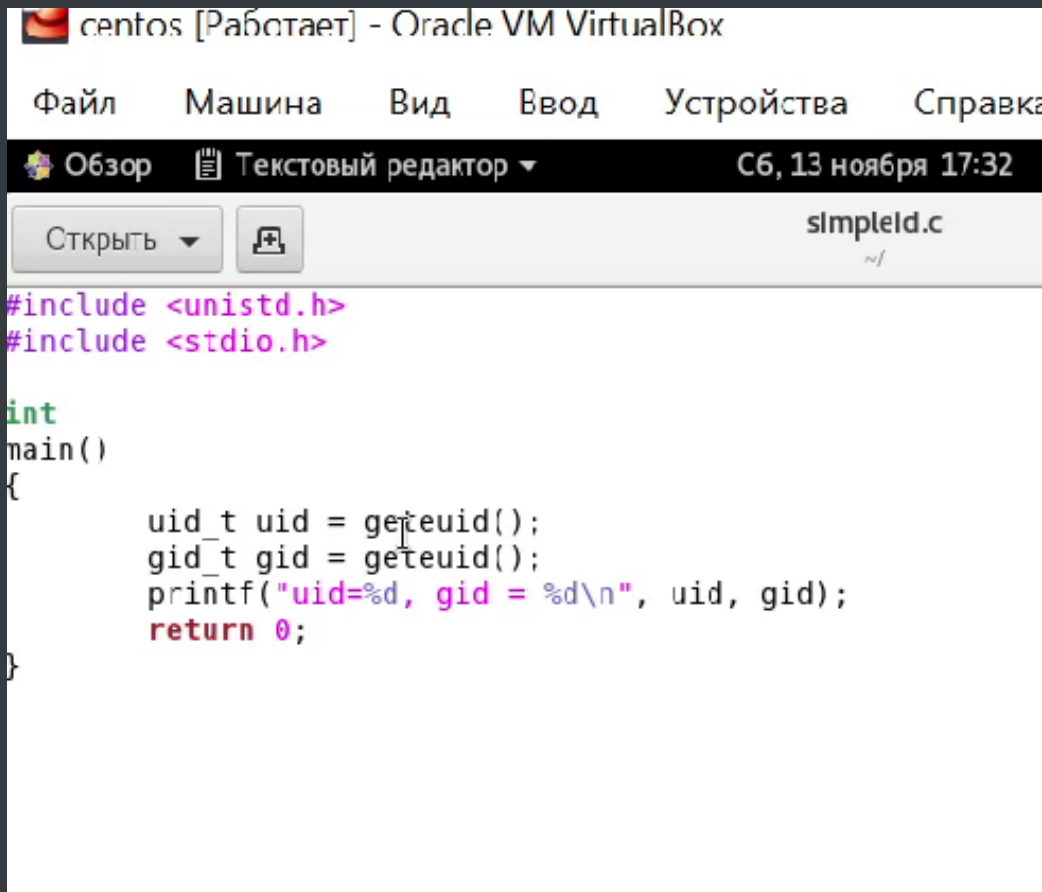
Группа: НФИбд-01-18

МОСКВА 2021г

Выполнение

1. Создание программы

От имени пользователя guest создали программу simpleid.c:



centos [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Обзор Текстовый редактор C6, 13 ноября 17:32

Скрыть simpleid.c

```
#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;
}
```

В установленной системе отсутствует библиотека types.h, поэтому пришлось удалить ее из кода

Выполнили программу simpleid и системную программу id

```
simpleid.c:1:10: фатальная ошибка: sys/types.h.: Нет такого файла или каталога
#include <sys/types.h>
      ^~~~~~
компиляция прервана.
[root@saloginov guest]# gcc simpleid.c -o simpleid
[root@saloginov guest]# ./simpleid
uid=0, gid = 0
[root@saloginov guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Результаты выполнения одинаковые

Усложнили программу, добавив вывод действительных идентификаторов

```

#include <unistd.h>
#include <stdio.h>

int
main()
{
    uid_t real_uid = getuid();
    uid_t uid = geteuid();
    gid_t real_gid = getegid();
    gid_t gid = getegid();
    printf("uid=%d, gid = %d\n", uid, gid);
    printf("real_uid = %d, real_gid = %d\n", real_uid, real_gid);
    return 0;
}

```

Запустили программу и сравнили вывод

```

[root@saloginov guest]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconf
ined_t:s0-s0:c0.c1023
[root@saloginov guest]# gcc simpleid.c -o simpleid
[root@saloginov guest]# ./simpleid
uid=0, gid = 0
real_uid = 0, real_gid = 0
[root@saloginov guest]#

```

От имени суперпользователя выполнили команды

chown root:guest /home/guest/simpleid2 - команда для смены владельца файла

chmod u+s /home/guest/simpleid2 - команда для изменения прав доступа файла

Выполнили проверку правильности установки новых атрибутов и смены владельца файла simpleid2:

ls -l simpleid2

```

[root@saloginov guest]# chown root:guest simpleid
[root@saloginov guest]# chmod u+s simpleid
[root@saloginov guest]# ls -l simpleid
-rwsr-xr-x. 1 root guest 17592 ноя 13 17:36 simpleid
[root@saloginov guest]#

```

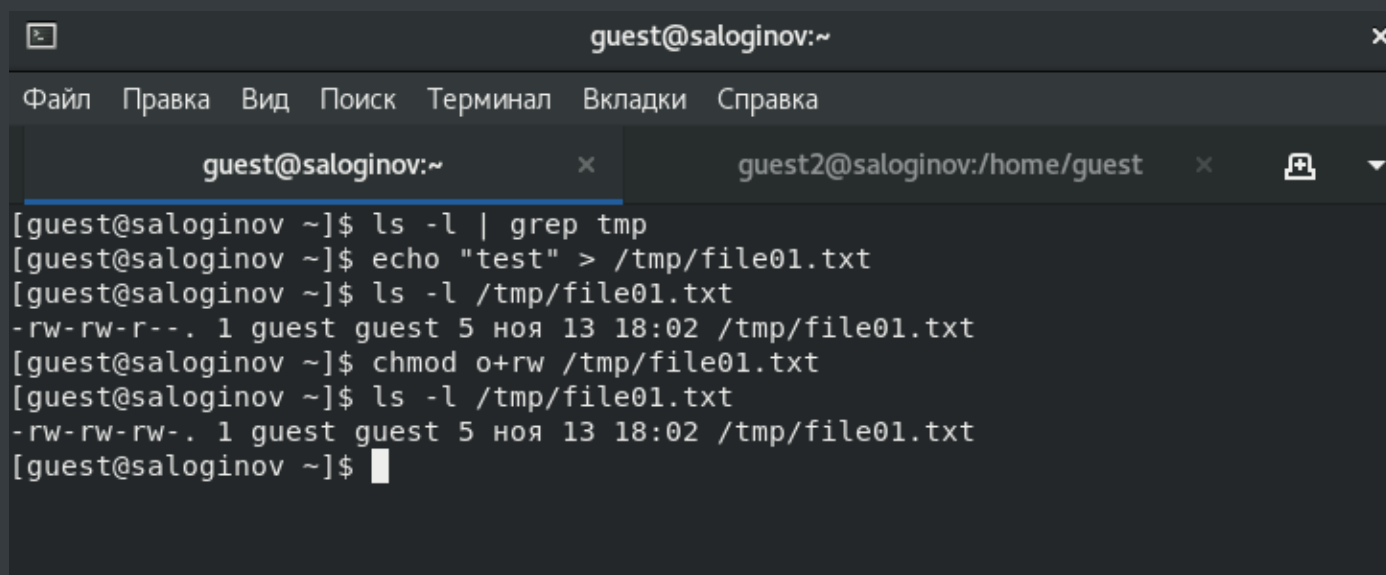
Программу readfile создать не удалось из-за проблем с библиотеками

2. Исследование Sticky-бита

Выяснили, что атрибут Sticky установлен на директории /tmp

От имени пользователя guest создали файл file01.txt в директории /tmp со словом test

Просмотрели атрибуты у только что созданного файла и разрешили чтение и запись для категории пользователей «все остальные»:



```
guest@saloginov:~  
Файл  Правка  Вид  Поиск  Терминал  Вкладки  Справка  
guest@saloginov:~ x guest2@saloginov:/home/guest x  
[guest@saloginov ~]$ ls -l | grep tmp  
[guest@saloginov ~]$ echo "test" > /tmp/file01.txt  
[guest@saloginov ~]$ ls -l /tmp/file01.txt  
-rw-rw-r--. 1 guest guest 5 ноя 13 18:02 /tmp/file01.txt  
[guest@saloginov ~]$ chmod o+rw /tmp/file01.txt  
[guest@saloginov ~]$ ls -l /tmp/file01.txt  
-rw-rw-rw-. 1 guest guest 5 ноя 13 18:02 /tmp/file01.txt  
[guest@saloginov ~]$
```

От пользователя guest2 (не являющегося владельцем) прочитали файл /tmp/file01.txt

От пользователя guest2 дозаписали в файл /tmp/file01.txt слово test2

От пользователя guest2 записали в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию

Попробовали удалить файл и получили отказ:

```
guest2@saloginov:/home/guest
Файл Правка Вид Поиск Терминал Вкладки Справка
guest@saloginov:~ x guest2@saloginov:/home/guest x
Пароль:
su: Сбой при проверке подлинности
[guest@saloginov ~]$ su guest2
Пароль:
[guest2@saloginov guest]$ cat /tmp/file01.txt
test
[guest2@saloginov guest]$ echo "test2" > tmp/file01.txt
bash: tmp/file01.txt: Нет такого файла или каталога
[guest2@saloginov guest]$ echo "test2" > /tmp/file01.txt
[guest2@saloginov guest]$ cat /tmp/file01.txt
test2
[guest2@saloginov guest]$ echo "test3" > /tmp/file01.txt
[guest2@saloginov guest]$ cat /tmp/file01.txt
test3
[guest2@saloginov guest]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
```

Повысили права до суперпользователя и сняли атрибут t с директории /tmp

Вышли из режима суперпользователя и повторили действия, теперь удаление прошло успешно

Вернули атрибут t на директорию /tmp

```
[guest2@saloginov guest]$ su
Пароль:
[root@saloginov guest]# chmod -t /tmp
[root@saloginov guest]# exit
exit
[guest2@saloginov guest]$ ls -l / |grep tmp
drwxrwxrwx. 21 root root 4096 ноя 13 18:07 tmp
[guest2@saloginov guest]$ echo "test4" > /tmp/file01.txt
[guest2@saloginov guest]$ cat /tmp/file01.txt
test4
[guest2@saloginov guest]$ rm /tmp/file01.txt
[guest2@saloginov guest]$ su
Пароль:
[root@saloginov guest]# chmod +t /tmp
[root@saloginov guest]# exit
exit
```