

Отчет по лабораторной работе №5

Основы информационной безопасности

Федоров Андрей

Российский университет дружбы народов, Москва, Россия

Информация

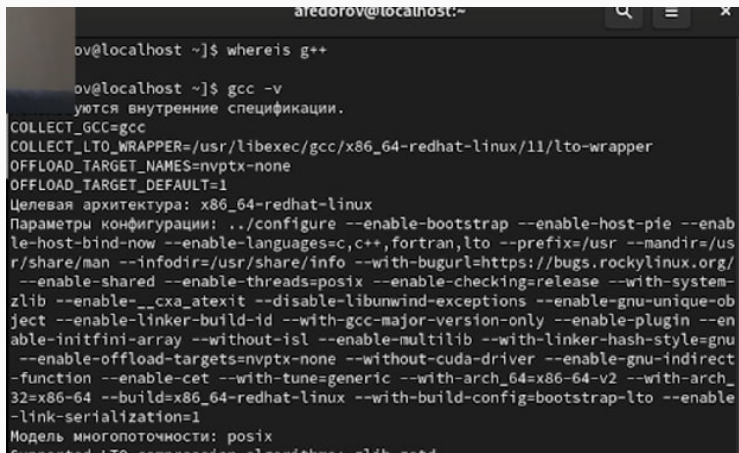
- Федоров Андрей Андреевич
- студент
- НБИ 2 курс
- Российский университет дружбы народов

- Даёт понять, о чём пойдёт речь
- Следует широко и кратко описать проблему
- Мотивировать свое исследование
- Сформулировать цели и задачи
- Возможна формулировка ожидаемых результатов

- Не формулируйте более 1–2 целей исследования

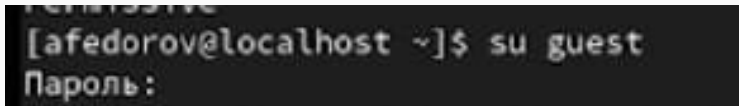
- Представляйте данные качественно
- Количественно, только если крайне необходимо
- Излишние детали не нужны

Для лабораторной работы необходимо проверить, установлен ли компилятор gcc, команда `gcc -v` позволяет это сделать. Также осуществляется отключение системы запретов с помощью `setenforce 0` (рис. 1).

A screenshot of a terminal window with a dark background. The prompt is 'aredorov@localhost:~'. The user has entered 'whereis g++' and 'gcc -v'. The output of 'gcc -v' shows various configuration options and the target architecture 'x86_64-redhat-linux'.

```
aredorov@localhost:~$ whereis g++
aredorov@localhost:~$ gcc -v
уются внутренние спецификации.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-redhat-linux/11/lto-wrapper
OFFLOAD_TARGET_NAMES=nvptx-none
OFFLOAD_TARGET_DEFAULT=1
Целевая архитектура: x86_64-redhat-linux
Параметры конфигурации: ./configure --enable-bootstrap --enable-host-pie --enable-host-bind-now --enable-languages=c,c++,fortran,lto --prefix=/usr --mandir=/usr/share/man --infodir=/usr/share/info --with-bugurl=https://bugs.rockylinux.org/ --enable-shared --enable-threads=posix --enable-checking=release --with-system-zlib --enable-_cxa_atexit --disable-libunwind-exceptions --enable-gnu-unique-object --enable-linker-build-id --with-gcc-major-version-only --enable-plugin --enable-initfini-array --without-isl --enable-multilib --with-linker-hash-style=gnu --enable-offload-targets=nvptx-none --without-cuda-driver --enable-gnu-indirect-function --enable-cet --with-tune=generic --with-arch_64=x86-64-v2 --with-arch_32=x86-64 --build=x86_64-redhat-linux --with-build-config=bootstrap-lto --enable-link-serialization=1
Модель многопоточности: posix
supported LTO compression algorithms: zlib gnu
```

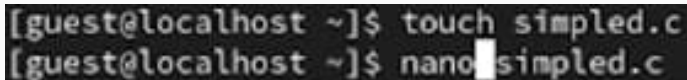
Осуществляется вход от имени пользователя guest (рис. 2).



```
terminal$ su guest  
[afedorov@localhost ~]$ su guest  
Пароль:
```

Рис. 2: Вход от имени пользователя guest

Создание файла `simplified.c` и запись в файл кода (рис. 3)

A terminal window with a black background and white text. The first line shows the command 'touch simplified.c' being executed. The second line shows the command 'nano simplified.c' being executed, with a white cursor visible at the end of the filename.

```
[guest@localhost ~]$ touch simplified.c  
[guest@localhost ~]$ nano simplified.c
```

Рис. 3: Создание файла

Содержимое файла выглядит следующти образом (рис. 4)

A screenshot of a code editor showing the content of a file named 'simple'. The code is written in C and includes headers for system types, unistd, and stdio. It defines a main function that calls geteuid and getegid to retrieve the effective user and group IDs, prints them using printf, and then returns 0. The code is color-coded: keywords like 'int', 'main', 'return', and 'printf' are in green, identifiers like 'uid_t', 'gid_t', 'uid', and 'gid' are in blue, and string literals and header names are in orange. The file name 'simple' is visible in the top right corner of the editor window.

```
ano 5.6.1 simple
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main()
[
    uid_t uid = geteuid ();
    gid_t git = getegit ();
    printf ("uid=%d, gid=%d\n", uid, gid);
    return 0;
]
```

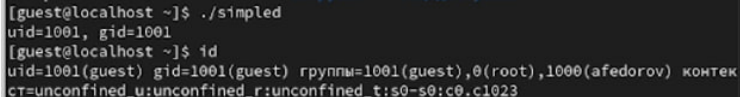
Рис. 4: Содержимое файла

Компилирую файл, проверяю, что он скомпилировался (рис. 5)

```
[guest@localhost ~]$ gcc simplified.c -o simplified
[guest@localhost ~]$ ls
dir!          simplified    Видео         Изображения   'Рабочий стол'
simple.c.save  simplified.c  Документы     Музыка         Шаблоны
simple.c.save.1 test         Загрузки     Общедоступные
```

Рис. 5: Компиляция файла

Запускаю исполняемый файл. В выводе файла выписаны номера пользователя и групп, от вывода при вводе `if`, они отличаются только тем, что информации меньше (рис. 6)



```
[guest@localhost ~]$ ./simplified
uid=1001, gid=1001
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) rpynm=1001(guest),0(root),1000(afedorov) контек
ст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 6: Сравнение команд

Создание, запись в файл и компиляция файла simple2.c. Запуск программы (рис. 7)

A terminal window with a black background and white text. The prompt is [guest@localhost ~]. The user enters three commands: touch simple2.c, nano simple2.c, and gcc simple2.c -o simple2. The output of the first two commands is not visible, but the prompt returns. The output of the third command is also not visible.

```
[guest@localhost ~]$ touch simple2.c  
[guest@localhost ~]$ nano simple2.c  
[guest@localhost ~]$ gcc simple2.c -o simple2
```

Рис. 7: Создание и компиляция файла



```
no 5.6.1                                simple2.c
<sys/types.h>
<unistd.h>
<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;
}
```

Рис. 8: Содержимое файла

С помощью `chown` изменяю владельца файла на суперпользователя, с помощью `chmod` изменяю права доступа (рис. 9)

```
[afedorov@localhost ~]$ sudo chown root:guest /home/guest/simple2
[sudo] пароль для afedorov:
[afedorov@localhost ~]$ sudo chmod u+s /home/guest/simple2
[afedorov@localhost ~]$ sudo ls -l /home/guest/simple2
-rwsr-xr-x. 1 root guest 17720 июн 17 23:47 /home/guest/simple2
[afedorov@localhost ~]$ sudo /home/guest/simple2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
```

Рис. 9: Смена владельца файла и прав доступа к файлу

Сравнение вывода программы и команды `id`, наша команда снова вывела только ограниченное количество информации(рис. 10)

```
[afedorov@localhost ~]$ sudo /home/guest/simple2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[afedorov@localhost ~]$ id
uid=1000(afedorov) gid=1000(afedorov) группы=1000(afedorov),10(wheel) контекст=u
nconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[afedorov@localhost ~]$ sudo id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconf
ined_t:s0-s0:c0.c1023
```

Рис. 10: Запуск файла

Создание и компиляция файла readfile.c (рис. 11)

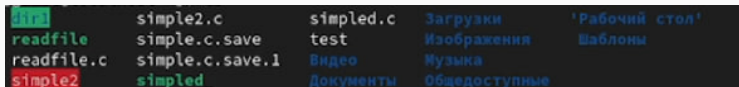


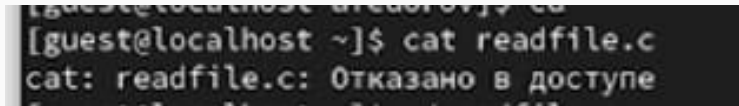
Рис. 11: Создание и компиляция файла

Снова от имени суперпользователя меняю владельца файла readfile. Далее меняю права доступа так, чтобы пользователь guest не смог прочесть содержимое файла (рис. 13)

```
[afedorov@localhost ~]$ sudo chmod u+s /home/guest/readfile.c  
[afedorov@localhost ~]$ sudo chmod 700 /home/guest/readfile.c  
[afedorov@localhost ~]$ sudo chmod -r /home/guest/readfile.c  
[afedorov@localhost ~]$ sudo chmod u+s /home/guest/readfile.c  
[afedorov@localhost ~]$ su guest
```

Рис. 12: Смена владельца файла и прав доступа к файлу

Проверка прочесть файл от имени пользователя guest. Прочесть файл не удастся (рис. 14)



```
[guest@localhost ~]$ cat readfile.c  
cat: readfile.c: Отказано в доступе
```

Рис. 13: Попытка прочесть содержимое файла

Попытка прочесть тот же файл с помощью программы readfile, в ответ получаем “отказано в доступе” (рис. 15)



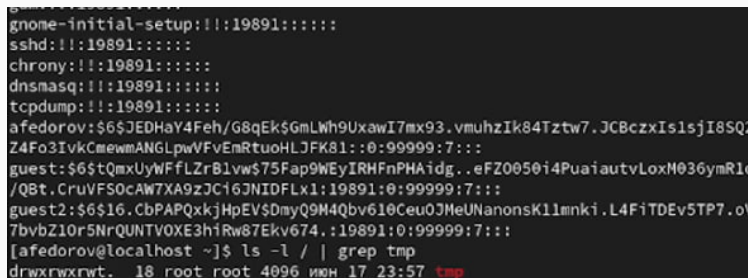
Рис. 14: Попытка прочесть содержимое файла программой

Попытка прочесть файл `\etc\shadow` с помощью программы, все еще получаем отказ в доступе (рис. 16)



Рис. 15: Попытка прочесть содержимое файла программой

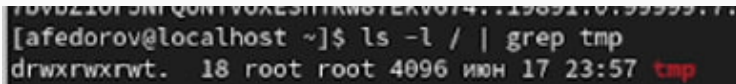
Пробуем прочесть эти же файлы от имени суперпользователя и чтение файлов проходит успешно (рис. 17)



```
gnome-initial-setup:!!:19891:~::~:
sshd:!!:19891:~::~:
chrony:!!:19891:~::~:
dnsmasq:!!:19891:~::~:
tcpdump:!!:19891:~::~:
afedorov:$6$JEDHaY4Feh/G8qEk$GmLWh9UxawI7mx93.vmuHzIk84Tztw7.JCBczxIs1sjI8SQ2
Z4Fo3IvkCmewmANGLpwVFvEmRtuoHLJFK81:::0:99999:7:::
guest:$6$tQmxUyWfFLZrB1vw$75Fap9WEyIRHFnPHAidg..eFZ0050i4PuaiautvLoxM036ymR1d
/QBt.CruVFS0cAW7XA9zJC16JNIDFLx1:19891:0:99999:7:::
guest2:$6$16.CbPAPQxkjHpEV$DmyQ9M4Qbv610Ceu0JMeUNanonsK1lmnki.L4FiTDEv5TP7.oV
7bvbZ10r5NrQUNTVOXE3h1Rw87Ekv674.:19891:0:99999:7:::
[afedorov@localhost ~]$ ls -l / | grep tmp
drwxrwxrwt. 18 root root 4096 июн 17 23:57 tmp
```

Рис. 16: Чтение файла от имени суперпользователя

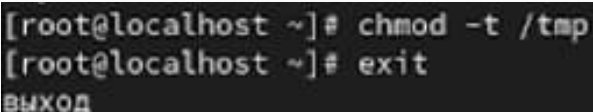
Проверяем папку tmp на наличие атрибута Sticky, т.к. в выводе есть буква t, то атрибут установлен (рис. 18)



```
FOV021013011Q0N1V0XES1TKW07EKV014.:19891.0.99999.7.  
[afedorov@localhost ~]$ ls -l / | grep tmp  
drwxrwxrwt. 18 root root 4096 июн 17 23:57 tmp
```

Рис. 17: Проверка атрибутов директории tmp

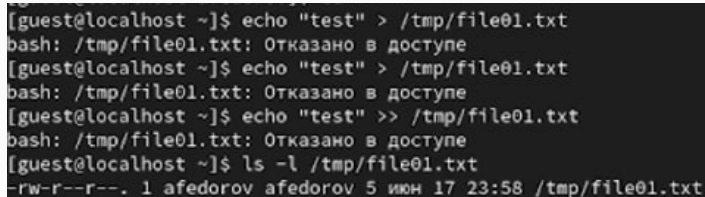
От имени пользователя guest создаю файл с текстом, добавляю права на чтение и запись для других пользователей (рис. 19)

A terminal window with a black background and white text. It shows two commands being executed: 'chmod -t /tmp' and 'exit'. The prompt is '[root@localhost ~]#'. Below the 'exit' command, the word 'выход' is written in white Cyrillic text.

```
[root@localhost ~]# chmod -t /tmp  
[root@localhost ~]# exit  
выход
```

Рис. 18: Создание файла, изменение прав доступа

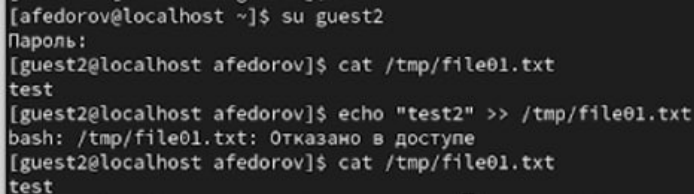
Вхожу в систему от имени пользователя guest2, от его имени могу прочитать файл file01.txt, но перезаписать информацию в нем не могу (рис. 20)

A terminal window showing a user named 'guest2' attempting to write to a file. The user runs 'echo "test" > /tmp/file01.txt' three times, each time receiving the error 'bash: /tmp/file01.txt: Отказано в доступе'. Finally, the user runs 'ls -l /tmp/file01.txt', which shows the file's permissions as '-rw-r--r--' and its owner as 'afedorov'.

```
[guest@localhost ~]$ echo "test" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest@localhost ~]$ echo "test" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest@localhost ~]$ echo "test" >> /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest@localhost ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 afedorov afedorov 5 июн 17 23:58 /tmp/file01.txt
```

Рис. 19: Попытка чтения файла

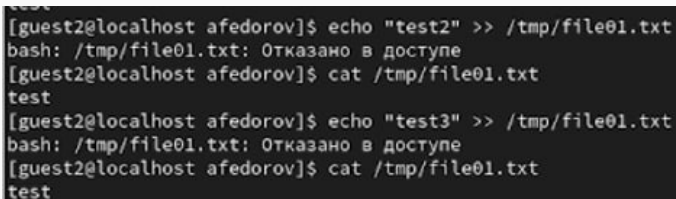
Также невозможно добавить в файл file01.txt новую информацию от имени пользователя guest2 (рис. 21)



```
[afedorov@localhost ~]$ su guest2
Пароль:
[guest2@localhost afedorov]$ cat /tmp/file01.txt
test
[guest2@localhost afedorov]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@localhost afedorov]$ cat /tmp/file01.txt
test
```

Рис. 20: Попытка записи в файл

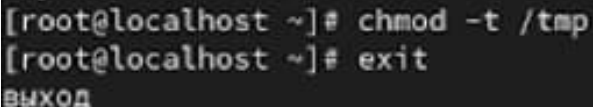
Далее пробуем удалить файл, снова получаем отказ (рис. 22)



```
test
[guest2@localhost afedorov]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@localhost afedorov]$ cat /tmp/file01.txt
test
[guest2@localhost afedorov]$ echo "test3" >> /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@localhost afedorov]$ cat /tmp/file01.txt
test
```

Рис. 21: Попытка удалить файл

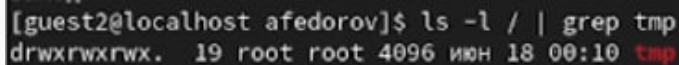
От имени суперпользователя снимаем с директории атрибут Sticky (рис. 23)



```
[root@localhost ~]# chmod -t /tmp  
[root@localhost ~]# exit  
выход
```

Рис. 22: Смена атрибутов файла

Проверяем, что атрибут действительно снят (рис. 24)



```
[guest2@localhost afedorov]$ ls -l / | grep tmp
drwxrwxrwx. 19 root root 4096 июн 18 00:10 tmp
```

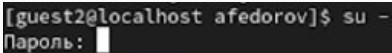
Рис. 23: Проверка атрибутов директории

Далее был выполнен повтор предыдущих действий. По результатам без Sticky-бита запись в файл и дозапись в файл осталась невозможной, зато удаление файла прошло успешно (рис. 25)

```
localhost afedorov]$ ls -l /home/guest
drwxrwxrwx. 4 guest guest  43 июн 17 23:24 .
-rwxr-xr-x. 1 guest guest 17664 июн 17 23:52 readfile
--ws-----. 1 root  guest  402 июн 17 23:52 readfile.c
-rwsr-xr-x. 1 root  guest 17720 июн 17 23:47 simple2
-rw-r--r--. 1 guest guest  303 июн 17 23:47 simple2.c
-rw-----. 1 guest guest   1 июн 17 23:14 simple.c.save
-rw-----. 1 guest guest   1 июн 17 23:14 simple.c.save.1
-rwxr-xr-x. 1 guest guest 17616 июн 17 23:44 simpled
-rw-r--r--. 1 guest guest  175 июн 17 23:44 simpled.c
-rw-r--r--. 1 guest guest   5 июн 17 21:35 test
drwxr-xr-x. 2 guest guest   6 июн 17 21:24 Видео
drwxr-xr-x. 2 guest guest   6 июн 17 21:24 Документы
drwxr-xr-x. 2 guest guest   6 июн 17 21:24 Загрузки
drwxr-xr-x. 2 guest guest   6 июн 17 21:24 Изображения
drwxr-xr-x. 2 guest guest   6 июн 17 21:24 Музыка
drwxr-xr-x. 2 guest guest   6 июн 17 21:24 Общедоступные
drwxr-xr-x. 2 guest guest   6 июн 17 21:24 'Рабочий стол'
drwxr-xr-x. 2 guest guest   6 июн 17 21:24 Шаблоны
```

Рис. 24: Повтор предыдущих действий

Возвращение директории tmp атрибута t от имени суперпользователя (рис. 26)



```
[guest2@localhost afedorov]$ su -  
Пароль: 
```

Рис. 25: Изменение атрибутов

- Изучил механизм изменения идентификаторов, применил SetUID- и Sticky-биты. Получил практические навыки работы в кон- соли с дополнительными атрибутами. Рассмотрел работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.