

Презентация по пятой лабораторной. Предмет - Информационная безопасность.

Попов Олег Павлович¹

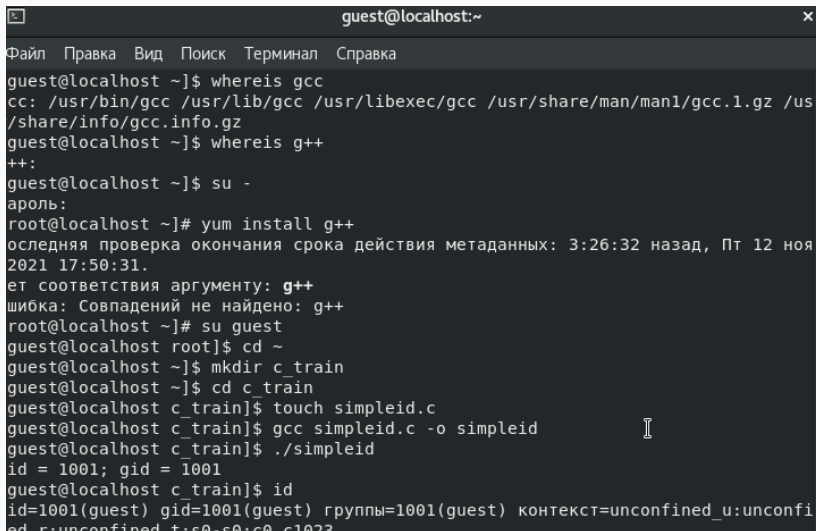
2021, 18 Сентября – 18 Сентября

¹RUDN University, Moscow, Russian Federation

Выполнение лабораторной

Выполнение команд

Компилятор gcc был установлен за кадром с помощью команды: `yum install gcc`.



```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
guest@localhost ~]$ whereis gcc  
cc: /usr/bin/gcc /usr/lib/gcc /usr/libexec/gcc /usr/share/man/man1/gcc.1.gz /us  
/share/info/gcc.info.gz  
guest@localhost ~]$ whereis g++  
++:  
guest@localhost ~]$ su -  
ароль:  
root@localhost ~)# yum install g++  
оследняя проверка окончания срока действия метаданных: 3:26:32 назад, Пт 12 ноя  
2021 17:50:31.  
ет соответствия аргументу: g++  
шибка: Совпадений не найдено: g++  
root@localhost ~)# su guest  
guest@localhost root]$ cd ~  
guest@localhost ~]$ mkdir c_train  
guest@localhost ~]$ cd c_train  
guest@localhost c_train]$ touch simpleid.c  
guest@localhost c_train]$ gcc simpleid.c -o simpleid  
guest@localhost c_train]$ ./simpleid  
id = 1001; gid = 1001  
guest@localhost c_train]$ id  
id=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ed_r:unconfined_t:s0-s0:c0-c1023
```

Выполнение лабораторной

```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
guest@localhost c_train]$ gcc simpleid2.c -o simpleid2  
guest@localhost c_train]$ ./simpleid2  
e_uid = 1001; e_gid = 1001  
real_uid = 1001; real_gid = 1001  
guest@localhost c_train]$ su -  
Пароль:  
root@localhost ~]# chown root:guest /home/guest/c_train/simple2  
chown: невозможно получить доступ к '/home/guest/c_train/simple2': Нет такого файла или каталога  
root@localhost ~]# chown root:guest /home/guest/c_train/simpleid2  
root@localhost ~]# chmod u+s /home/guest/c_train/simpleid2  
root@localhost ~]# lsattr /home/guest/c_train/simpleid2  
----- /home/guest/c_train/simpleid2  
root@localhost ~]# ls -l simpleid2  
ls: невозможно получить доступ к 'simpleid2': Нет такого файла или каталога  
root@localhost ~]# su guest  
guest@localhost root]$ cd ~/c_train  
guest@localhost c_train]$ ls -l simpleid2  
-rwsrwxr-x. 1 root guest 17648 ноя 12 21:29 simpleid2  
guest@localhost c_train]$ su -  
Пароль:  
root@localhost ~]# chmod +d /home/guest/c_train/simpleid2  
chmod: неверный режим: «+d»  
по команде «chmod --help» можно получить дополнительную информацию.
```

Выполнение лабораторной

```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[root@localhost ~]# chmod u+d /home/guest/c_train/simpleid2  
chmod: неверный режим: «u+d»  
По команде «chmod --help» можно получить дополнительную информацию.  
[root@localhost ~]# chmod d /home/guest/c_train/simpleid2  
chmod: неверный режим: «d»  
По команде «chmod --help» можно получить дополнительную информацию.  
[root@localhost ~]# ls -ld /home/guest/c_train/simpleid2  
-rwsrwxr-x. 1 root guest 17648 ноя 12 21:29 /home/guest/c_train/simpleid2  
[root@localhost ~]# chmod g+s /home/guest/c_train/simpleid2  
[root@localhost ~]# ls -ld /home/guest/c_train/simpleid2  
-rwsrwsr-x. 1 root guest 17648 ноя 12 21:29 /home/guest/c_train/simpleid2  
[root@localhost ~]# su guest  
[guest@localhost root]$ cd ~/c_train  
[guest@localhost c_train]$ touch readfile.c  
[guest@localhost c_train]$ gcc readfile.c -o readfile  
readfile.c:1:10: фатальная ошибка: fcntl.h: Нет такого файла или каталога  
#include <fcntl.h>  
~~~~~  
компиляция прервана.  
[guest@localhost c_train]$ gcc readfile.c -o readfile  
readfile.c:1:10: фатальная ошибка: fnctl.h: Нет такого файла или каталога  
#include <fnctl.h>  
~~~~~  
компиляция прервана.
```

Выполнение лабораторной

```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@localhost c_train]$ gcc readfile.c -o readfile  
readfile.c:1:10: фатальная ошибка: funct1.h: Нет такого файла или каталога  
#include <funct1.h>  
      ^~~~~~  
компиляция прервана.  
[guest@localhost c_train]$ yum install fnct1.h  
Ошибка: Эту команду нужно запускать с привилегиями суперпользователя (на большин  
стве систем - под именем пользователя root).  
[guest@localhost c_train]$ su -  
Пароль:  
[root@localhost ~]# yum install fnct1.h  
Последняя проверка окончания срока действия метаданных: 0:13:51 назад, Пт 12 ноя  
2021 21:34:10.  
Нет соответствия аргументу: fnct1.h  
Ошибка: Совпадений не найдено: fnct1.h  
[root@localhost ~]# su guest  
[guest@localhost root]$ cd ~/c_train  
[guest@localhost c_train]$ gcc readfile.c -o readfile  
readfile.c: В функции «main»:  
readfile.c:8:2: ошибка: «unsigned» не описан (первое использование в этой функции  
)  
  unsigned char buffer[16];  
  ^~~~~~  
readfile.c:8:2: замечание: сообщение о каждом неопisanном идентификаторе выдается
```

Выполнение лабораторной

```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
я один раз в каждой функции, где он встречается  
readfile.c:8:9: ошибка: expected «;» before «char»  
    unsigned char buffer[16];  
    ^~~~~~  
;  
readfile.c:12:20: ошибка: индексруемый объект не является ни массивом, ни указателем, ни вектором  
    int fd = open(argc[1], O_RDONLY);  
    ^  
readfile.c:14:25: ошибка: «buffer» не описан (первое использование в этой функции); имелось в виду «setbuffer»?  
    bytes_read = read(fd, buffer, sizeof(buffer));  
    ^~~~~~  
    setbuffer  
[guest@localhost c_train]$ gcc readfile.c -o readfile  
readfile.c: В функции «main»:  
readfile.c:12:20: ошибка: индексруемый объект не является ни массивом, ни указателем, ни вектором  
    int fd = open(argc[1], O_RDONLY);  
    ^  
[guest@localhost c_train]$ gcc readfile.c -o readfile  
[guest@localhost c_train]$ su -  
Пароль:  
[root@localhost ~]# chown root /home/guest/c_train/readfile.c
```

Выполнение лабораторной

[illegible]

Выполнение лабораторной

```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[00] 5x[0000000000000000] guest@localhost c_train]$ 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 c_train]$ su -  
Пароль:
```

Выполнение лабораторной

[illegible]

Выполнение лабораторной

Теперь переходим к части со Sticky bit.

```
guest@localhost:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
gz=38;5;9:*.lrz=38;5;9:*.lz=38;5;9:*.lzo=38;5;9:*.xz=38;5;9:*.zst=38;5;9:*.tztst  
=38;5;9:*.bz2=38;5;9:*.bz=38;5;9:*.tbz=38;5;9:*.tbz2=38;5;9:*.tz=38;5;9:*.deb=38  
;5;9:*.rpm=38;5;9:*.jar=38;5;9:*.war=38;5;9:*.ear=38;5;9:*.sar=38;5;9:*.rar=38;5  
;9:*.alz=38;5;9:*.ace=38;5;9:*.zoo=38;5;9:*.cpio=38;5;9:*.7z=38;5;9:*.rz=38;5;9:  
*.cab=38;5;9:*.wim=38;5;9:*.swm=38;5;9:*.dwm=38;5;9:*.esd=38;5;9:*.jpg=38;5;13:*.  
jpeg=38;5;13:*.mjpg=38;5;13:*.mjpeg=38;5;13:*.gif=38;5;13:*.bmp=38;5;13:*.pbm=3  
8;5;13:*.pgm=38;5;13:*.ppm=38;5;13:*.tga=38;5;13:*.xbm=38;5;13:*.xpm=38;5;13:*.t  
if=38;5;13:*.tiff=38;5;13:*.png=38;5;13:*.svg=38;5;13:*.svgz=38;5;13:*.mng=38;5;  
13:*.pcx=38;5;13:*.mov=38;5;13:*.mpg=38;5;13:*.mpeg=38;5;13:*.m2v=38;5;13:*.mkv=  
38;5;13:*.webm=38;5;13:*.ogm=38;5;13:*.mp4=38;5;13:*.m4v=38;5;13:*.mp4v=38;5;13:  
*.vob=38;5;10ошибка сегментирования (стек памяти сброшен на диск)  
[root@localhost ~]# su guest  
[guest@localhost root]$ cd ~  
[guest@localhost ~]$ ls -l / | grep tmp  
drwxrwxrwt. 13 root root 4096 ноя 12 22:03 tmp  
[guest@localhost ~]$ cd tmp  
bash: cd: tmp: Нет такого файла или каталога  
[guest@localhost ~]$ echo "test" > /tmp/file01.txt  
[guest@localhost ~]$ ls -l /tmp/file01.txt  
-rw-rw-r--. 1 guest guest 5 ноя 12 22:08 /tmp/file01.txt  
[guest@localhost ~]$ chmod o+rw /tmp/file01.txt  
[guest@localhost ~]$ ls -l /tmp/file01.txt  
-rw-rw-rw-. 1 guest guest 5 ноя 12 22:08 /tmp/file01.txt  
[guest@localhost ~]$
```

Выполнение лабораторной

```
guest2@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@localhost ~]$ su guest2  
Пароль:  
[guest2@localhost guest]$ cd ~  
[guest2@localhost ~]$ cat /tmp/file01.txt  
test  
[guest2@localhost ~]$ echo "test2" > /tmp/file01.txt  
[guest2@localhost ~]$ cat /tmp/file01.txt  
test2  
[guest2@localhost ~]$ echo "test3" > /tmp/file01.txt  
[guest2@localhost ~]$ cat /tmp/file01.txt  
test3  
[guest2@localhost ~]$ rm /tmp/file01.txt  
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена  
[guest2@localhost ~]$ su -  
Пароль:  
[root@localhost ~]# chmod -t /tmp  
[root@localhost ~]# exit  
выход  
[guest2@localhost ~]$ ls -l / | grep tmp  
bash: grep: команда не найдена...  
Аналогичная команда: 'grep'  
[guest2@localhost ~]$ ls -l / | grep tmp  
drwxrwxrwx. 13 root root 4096 ноя 12 22:12 tmp  
[guest2@localhost ~]$ cat /tmp/file01.txt
```

Выполнение лабораторной

```
guest2@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[guest2@localhost ~]$ rm /tmp/file01.txt  
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена  
[guest2@localhost ~]$ su -  
Пароль:  
[root@localhost ~]# chmod -t /tmp  
[root@localhost ~]# exit  
выход  
[guest2@localhost ~]$ ls -l / | grip tmp  
bash: grip: команда не найдена...  
Аналогичная команда: 'grep'  
[guest2@localhost ~]$ ls -l / | grep tmp  
drwxrwxrwx. 13 root root 4096 ноя 12 22:12 tmp  
[guest2@localhost ~]$ cat /tmp/file01.txt  
test3  
[guest2@localhost ~]$ echo "test2" > /tmp/file01.txt  
[guest2@localhost ~]$ cat /tmp/file01.txt  
test2  
[guest2@localhost ~]$ rm /tmp/file01.txt  
[guest2@localhost ~]$ su -  
Пароль:  
[root@localhost ~]# chmod +t /tmp  
[root@localhost ~]# exit  
выход  
[guest2@localhost ~]$
```

В итоге получается, что у пользователей вне группы `quest` есть права на запись и чтение файла, но при этом, если у директории `tmp` есть `Sticky bit`, удаление `file01` запрещено.