HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA CÔNG NGHỆ THÔNG TIN

Học phần: **Kỹ thuật xâm nhập**

Thực hành:
Bài Thực hành số 2

Giảng viên hướng dẫn: Nguyễn Ngọc Diệp
Sinh viên thực hiện:
Đỗ Quang Huy B18DCAT106

Hà Nội 2022

Bài 3 : GDB – Lesson

Start lab

```
student@ubuntu:~/labtainer/labtainer-student$ labtainer gdblesson
non-network local connections being added to access control list
Started 1 containers, 1 completed initialization. Done.



The lab manual is at
   file:///home/student/labtainer/trunk/labs/gdblesson/docs/gdblesson.pdf

You may open the manual by right clicking
and select "Open Link".


Press <enter> to start the lab

student@ubuntu:~/labtainer/labtainer-student$
```

Mở code samplemath.c

```
ubuntu@gdblesson: ~
File  Edit  View  Search  Terminal  Help



#include <stdio.h>
void main() {
    int num;
    int count;
    int total;
    total = 0;
    num = 6;
    count = 15;
    while(count > 0) { /* Modify this line only */
        total = count / num;
        printf("%d divided by %d is: %d\n", count, num, total);
        count--;
        num--;
    }
}
sampleMath.c (END)
```

Biên dịch và chạy thử

```
ubuntu@gdblesson: ~
File  Edit  View  Search  Terminal  Help
ubuntu@gdblesson:~$ ls
sampleMath  sampleMath.c  sampleMath2.c
ubuntu@gdblesson:~$ less sampleMath.c
ubuntu@gdblesson:~$ gcc -g sampleMath.c -o sampleMath
ubuntu@gdblesson:~$ ./sampleMath
15 divided by 6 is: 2
14 divided by 5 is: 2
13 divided by 4 is: 3
12 divided by 3 is: 4
11 divided by 2 is: 5
10 divided by 1 is: 10
Floating point exception (core dumped)
ubuntu@gdblesson:~$
```

Debug bằng gdb

```
ubuntu@gdblesson:~$ gdb sampleMath
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.5) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from sampleMath...done.
(gdb) run
Starting program: /home/ubuntu/sampleMath
15 divided by 6 is: 2
14 divided by 5 is: 2
13 divided by 4 is: 3
12 divided by 3 is: 4
11 divided by 2 is: 5
10 divided by 1 is: 10

Program received signal SIGFPE, Arithmetic exception.
0x0000000000400549 in main () at sampleMath.c:10
10              total = count / num;
(gdb)
```

Nhận thấy rằng lỗi ở dòng 10 vì khi num = 0 thì vòng lặp vẫn xảy ra nhưng lại không thể chia 0 được .

```
(gdb) list
5           int total;
6           total = 0;
7           num = 6;
8           count = 15;
9           while(count > 0) { /* Modify this line only */
10              total = count / num;
11              printf("%d divided by %d is: %d\n", count, num, total);
12              count--;
13              num--;
14          }
(gdb)
```

```
ubuntu@gdblesson: ~
File  Edit  View  Search  Terminal  Help
(gdb) list
5           int total;
6           total = 0;
7           num = 6;
8           count = 15;
9           while(count > 0) { /* Modify this line only */
10              total = count / num;
11              printf("%d divided by %d is: %d\n", count, num, total);
12              count--;
13              num--;
14          }
(gdb) break9
Undefined command: "break9".  Try "help".
(gdb) break 9
Breakpoint 1 at 0x400543: file sampleMath.c, line 9.
(gdb) r
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/ubuntu/sampleMath

Breakpoint 1, main () at sampleMath.c:9
9           while(count > 0) { /* Modify this line only */
(gdb) p
The history is empty.
(gdb)
```

Bắt đầu sửa code có thể sử dụng Nano hoặc Vim mình dùng Nano

Sửa count >0 thành num>0

Save file dùng tổ hợp Ctrl x + y + Enter .

```
ubuntu@gdblesson: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 2.5.3                File: sampleMath.c                          Modified

#include <stdio.h>
void main() {
    int num;
    int count;
    int total;
    total = 0;
    num = 6;
    count = 15;
    while(num > 0) { /* Modify this line only */
        total = count / num;
        printf("%d divided by %d is: %d\n", count, num, total);
        count--;
        num--;
    }
}

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     ^Y Prev Page
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  ^V Next Page
```

Biên dịch lại

Chạy lại và xem lại kết quả .

```
ubuntu@gdblesson: ~
File  Edit  View  Search  Terminal  Help
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
"/home/ubuntu/sampleMath.c": not in executable format: File format not recognized
(gdb) q
ubuntu@gdblesson:~$ nano sampleMath.c
ubuntu@gdblesson:~$ gcc -g sampleMath.c -o sampleMath
ubuntu@gdblesson:~$ ./sampleMath
15 divided by 6 is: 2
14 divided by 5 is: 2
13 divided by 4 is: 3
12 divided by 3 is: 4
11 divided by 2 is: 5
10 divided by 1 is: 10
ubuntu@gdblesson:~$
```

Biên dich sampleMath2.c

```
ubuntu@gdblesson:~$ gcc -g sampleMath2.c -o sampleMath2
ubuntu@gdblesson:~$ ./sampleMath2
You must provide one integer argument greater than 0.
The result of 1 should be 3.
The result of 2 should be 7.
The result of 3 should be 14.
The result of 4 should be 22.
Your total is: 32764
ubuntu@gdblesson:~$
l address:  [huydq.B18AT106@stu.ptit.edu.vn]
```

Chạy debug nhận ra rằng chưa khai báo biến total

```
ubuntu@gdblesson: ~
File  Edit  View  Search  Terminal  Help
8
9           /* Add line above      */
10          if(argc > 1) {
(gdb) $1
Undefined command: "$1".  Try "help".
(gdb) break 25
Breakpoint 1 at 0x400633: file sampleMath2.c, line 25.
(gdb) r
Starting program: /home/ubuntu/sampleMath2
You must provide one integer argument greater than 0.

Breakpoint 1, main (argc=1, argv=0x7fffffffe698) at sampleMath2.c:25
25          total = abs(total);
(gdb) p total
$1 = 32767
(gdb) break 4
Breakpoint 2 at 0x4005c5: file sampleMath2.c, line 4.
(gdb) r
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/ubuntu/sampleMath2

Breakpoint 2, main (argc=1, argv=0x7fffffffe698) at sampleMath2.c:10
10          if(argc > 1) {
(gdb)
```

Tiếp tục sửa bằng nano .

```
ubuntu@gdblesson: ~
File  Edit  View  Search  Terminal  Help
 GNU nano 2.5.3                File: sampleMath2.c                        Modified

include <stdio.h>
include <stdlib.h>
oid main(int argc, char *argv[]) {
    int total;
    int n;
    int i;
    /* Your edit goes below */
        total=0;
    /* Add line above      */
    if(argc > 1) {
        i = atoi(argv[1]);
    }
    else {
        printf("You must provide one integer argument greater than 0.\n");
        i = -1;
    }
    for(n = 0; n <= i; n++) {
        if(n % 2 == 0){
            total += (n + n + 1) * n;
        }

G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos
X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line
```

Chạy và nhận lại kết quả .

```
ubuntu@gdblesson: ~
File  Edit  View  Search  Terminal  Help
        Inferior 1 [process 457] will be killed.

Quit anyway? (y or n) y
ubuntu@gdblesson:~$ nano sampleMath2.c
ubuntu@gdblesson:~$ gcc -g sampleMath2.c -o sampleMath2
ubuntu@gdblesson:~$ ./sampleMath2
You must provide one integer argument greater than 0.
The result of 1 should be 3.
The result of 2 should be 7.
The result of 3 should be 14.
The result of 4 should be 22.
Your total is: 0
ubuntu@gdblesson:~$ ./sampleMath2 3
The result of 1 should be 3.
The result of 2 should be 7.
The result of 3 should be 14.
The result of 4 should be 22.
Your total is: 14
ubuntu@gdblesson:~$ ./sampleMath2 12
The result of 1 should be 3.
The result of 2 should be 7.
The result of 3 should be 14.
The result of 4 should be 22.
Your total is: 162
ubuntu@gdblesson:~$ ./sampleMath2 99
```

Bài 2 gdb-cpp

Biên dịch và chạy thử file main.cc

```
ubuntu@gdb-cpp: ~
File  Edit  View  Search  Terminal  Help
Makefile  main.cc
ubuntu@gdb-cpp:~$ g++ -ggdb -Wall -o main main.cc
ubuntu@gdb-cpp:~$ ls
Makefile  main  main.cc
ubuntu@gdb-cpp:~$ ./main
Creating Node, 1 are in existence right now
Creating Node, 2 are in existence right now
Creating Node, 3 are in existence right now
Creating Node, 4 are in existence right now
The fully created list is:
4
3
2
1

Now removing elements:
Creating Node, 5 are in existence right now
Destroying Node, 4 are in existence right now
4
3
2
1

Segmentation fault (core dumped)
ubuntu@gdb-cpp:~$
```

Chạy trên gdb .

```
ubuntu@gdb-cpp: ~
File  Edit  View  Search  Terminal  Help
(gdb) r
Starting program: /home/ubuntu/main
Creating Node, 1 are in existence right now
Creating Node, 2 are in existence right now
Creating Node, 3 are in existence right now
Creating Node, 4 are in existence right now
The fully created list is:
4
3
2
1

Now removing elements:
Creating Node, 5 are in existence right now
Destroying Node, 4 are in existence right now
4
3
2
1


Program received signal SIGSEGV, Segmentation fault.
0x000055555555586c in Node<int>::next (this=0x0) at main.cc:28
28        Node<T>* next () const { return next_; }
(gdb)
```

Các điểm ngắt có điều kiện

```
Program received signal SIGSEGV, Segmentation fault.
0x000055555555586c in Node<int>::next (this=0x0) at main.cc:28
28        Node<T>* next () const { return next_; }
(gdb) backtrack
Undefined command: "backtrack".  Try "help".
(gdb) backtrace
#0  0x000055555555586c in Node<int>::next (this=0x0) at main.cc:28
#1  0x0000555555555763 in LinkedList<int>::remove (this=0x55555556aeb0,
    item_to_remove=@0x7fffffffe43c: 1) at main.cc:77
#2  0x00005555555553b1 in main (argc=1, argv=0x7fffffffe558) at main.cc:120
(gdb)
```

```
(gdb) break 52
Breakpoint 1 at 0x5555555555f9: file main.cc, line 52.
(gdb)
```

Debug code :

```
Now removing elements:

Breakpoint 1, LinkedList<int>::remove (this=0x55555556aeb0,
    item_to_remove=@0x7fffffffe43c: 4) at main.cc:52
52          Node<T> *marker = head_;
(gdb) step.gdb
Undefined command: "step.gdb".  Try "help".
(gdb) step
53          Node<T> *temp = 0;  // temp points to one behind as we iterate
(gdb) step
55          while (marker != 0) {
(gdb) step
56            if (marker->value() == item_to_remove) {
(gdb) step
Node<int>::value (this=0x7ffff7f1344e <std::ostream::put(char)+94>)
    at main.cc:30
30        const T& value () const { return value_; }
(gdb) step
LinkedList<int>::remove (this=0x55555556aeb0,
    item_to_remove=@0x7fffffffe43c: 4) at main.cc:57
57              if (temp == 0) { // marker is the first element in the list
(gdb) step
58                if (marker->next() == 0) {
(gdb) step
```

Giải quyết lỗi bằng cách xóa maker = 0 ;

```
ubuntu@gdb-cpp: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 4.8                                    main.cc
            head_ = new Node<T>(marker->value(), marker->next());
            delete marker;
            marker = 0;
          }
          return 0;
        } else {
          temp->next (marker->next());
          delete temp;
          temp = 0;
          return 0;
        }
      }
//      marker = 0;  // reset the marker
      temp = marker;
      marker = marker->next();
    }

    return -1;  // failure
  }

  void print (void) {

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

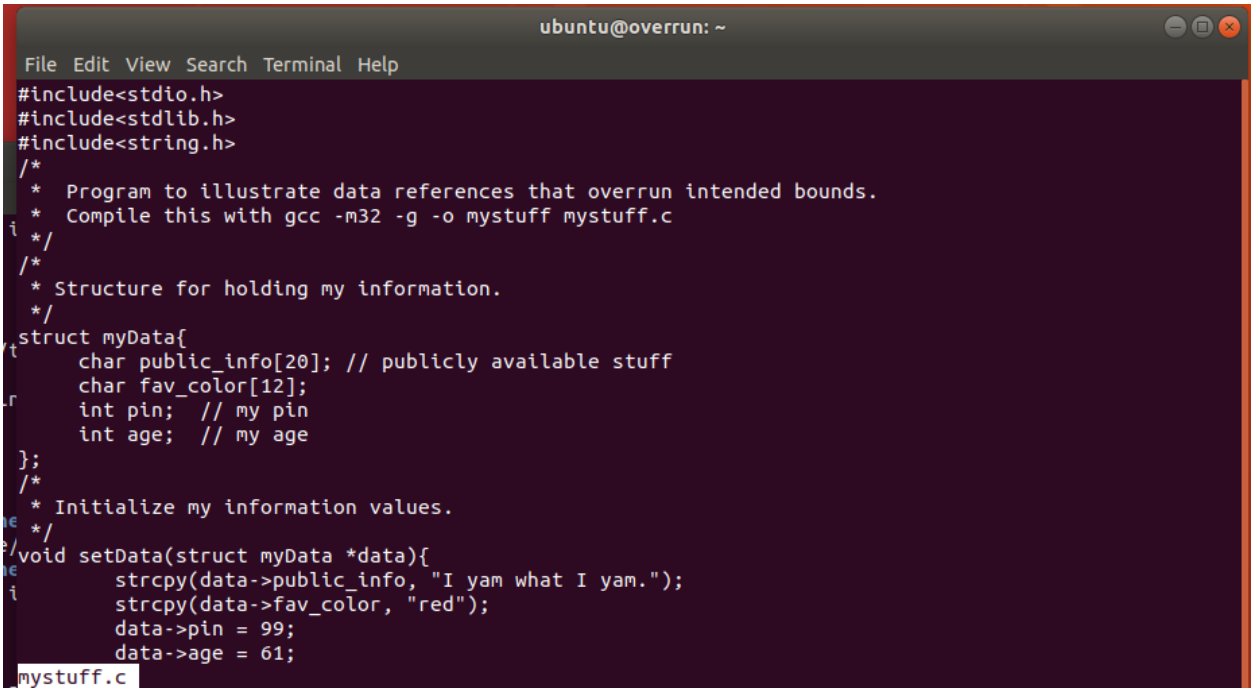
Chạy lại và nhận lại kết quả

```
ubuntu@gdb-cpp: ~
File  Edit  View  Search  Terminal  Help
Creating Node, 1 are in existence right now
Creating Node, 2 are in existence right now
Creating Node, 3 are in existence right now
Creating Node, 4 are in existence right now
The fully created list is:
4
3
2
1

Now removing elements:
Creating Node, 5 are in existence right now
Destroying Node, 4 are in existence right now
4
3
2
1

Destroying Node, 3 are in existence right now
4
3
1848857408
2

Destroying Node, 2 are in existence right now
```

Bài 3 overrun

Xem file mystuff.c

Bằng lệnh less mystuff.c .



Biên dịch và chạy thử

```
ubuntu@overrun:~$ gcc -m32 -g -o mystuff mystuff.c
ubuntu@overrun:~$ ./mystuff
Adress of public data:          0x0xffa4b0e4
Address of secret PIN:          0x0xffa4b104


Public data is I yam what I yam.
Hex value of PIN is 0x63


Enter an offset into your public data and we'll show you the character value.
(or q to quit)


22
22
Hex value at offset 22 (address 0x0xffa4b0c6) is 0x64
Enter an offset into your public data and we'll show you the character value.
(or q to quit)
64
64
Hex value at offset 64 (address 0x0xffa4b0f0) is 0x20
Enter an offset into your public data and we'll show you the character value.
(or q to quit)
11111111111111111111
11111111111111111111
Segmentation fault (core dumped)
ubuntu@overrun:~$
```

Có vẻ lỗi giống bài gdblesson .

Debug = gdb

```
(gdb) list
45          /* Initialized my_data */
46          setData(&my_data);
47
48          /* Display address of my_data fields */
49          printf("Adress of public data:\t\t0x%p\nAddress of secret PIN:\t\t0x%p\n", &my_data.publ
ic_info[0], &my_data.pin);
50          printf("\n\n");
51
52          /* Display values of my_data fields */
53          printf("Public data is %s\n",  my_data.public_info);
54          printf("Hex value of PIN is 0x%x\n", my_data.pin);
(gdb) show memory
Undefined show command: "memory".  Try "help show".
(gdb) showMemory
Undefined command: "showMemory".  Try "help".
(gdb) list showMemory
22              strcpy(data->fav_color, "red");
23              data->pin = 99;
24              data->age = 61;
25      }
26
27      void showMemory(struct myData data){
28          /* temporary variables */
29          int offset;
30          int result;
31          /* Show memory values at offsets into the public data field */
```

Break và xem data .

```
(gdb) break 38
Breakpoint 1 at 0x12d7: file mystuff.c, line 38.
(gdb) run
Starting program: /home/ubuntu/mystuff
Adress of public data:          0x0xffffd564
Address of secret PIN:          0x0xffffd584


Public data is I yam what I yam.
Hex value of PIN is 0x63


Enter an offset into your public data and we'll show you the character value.
(or q to quit)
10
10
```

Xem data.

```
Breakpoint 1, showMemory (data=...) at mystuff.c:38
38              printf("Hex value at offset %d (address 0x%p) is 0x%x\n", offset, &data.public_info[offset], data.public_info[offset]);
(gdb) x/10x &data
0xffffd530:     0x61792049      0x6877206d      0x49207461      0x6d617920
0xffffd540:     0xf7fe002e      0x00646572      0xf7e10212      0xf7fbf3fc
0xffffd550:     0x00000063      0x0000003d
(gdb) x/50x &data
0xffffd530:     0x61792049      0x6877206d      0x49207461      0x6d617920
0xffffd540:     0xf7fe002e      0x00646572      0xf7e10212      0xf7fbf3fc
0xffffd550:     0x00000063      0x0000003d      0xffffd584      0xffffd564
0xffffd560:     0x00000000      0x61792049      0x6877206d      0x49207461
0xffffd570:     0x6d617920      0xf7fe002e      0x00646572      0xf7e10212
0xffffd580:     0xf7fbf3fc      0x00000063      0x0000003d      0x23dc9a00
0xffffd590:     0x00000001      0x56558fcc      0xffffd5a8      0x56556416
0xffffd5a0:     0xffffd5c0      0x00000000      0x00000000      0xf7df6ee5
0xffffd5b0:     0xf7fbf000      0xf7fbf000      0x00000000      0xf7df6ee5
0xffffd5c0:     0x00000001      0xffffd654      0xffffd65c      0xffffd5e4
0xffffd5d0:     0xf7fbf000      0xf7ffd000      0xffffd638      0x00000000
0xffffd5e0:     0xf7ffd990      0x00000000      0xf7fbf000      0xf7fbf000
0xffffd5f0:     0x00000000      0x0499b140
(gdb)
```