

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**BÁO CÁO BÀI THỰC HÀNH**

**Kiểm thử xâm nhập**

Buffer overflow: 64 bit application

**Giảng viên: Đinh Trường Duy**

**Nhóm lớp: 02**

**Sinh viên: Nguyễn Trần Minh**

**Mã sinh viên: B20DCAT126**

**Hà Nội – 2024**

**Mục lục**

[**1. Mục đích 3**](#_Toc166827194)

[**2. Yêu cầu đối với sinh viên 3**](#_Toc166827195)

[**3. Nội dung thực hành 3**](#_Toc166827196)

[**4. Checkwork. 6**](#_Toc166827197)

# **Mục đích**

Bài thực hành Bufoverflow đã giới thiệu cho sinh viên về các lỗ hổng tràn bộ đệm và các cách khai thác của những lỗ hổng đó. Bài thực hành Bufoverflow bao gồm một chương trình có lỗ hổng chạy như một ứng dụng x86 32-bit. Bài thực hành này bao gồm cùng mã nguồn của chương trình có lỗ hổng, tuy nhiên nó được biên dịch và chạy như một ứng dụng 64-bit.

1. **Yêu cầu đối với sinh viên**

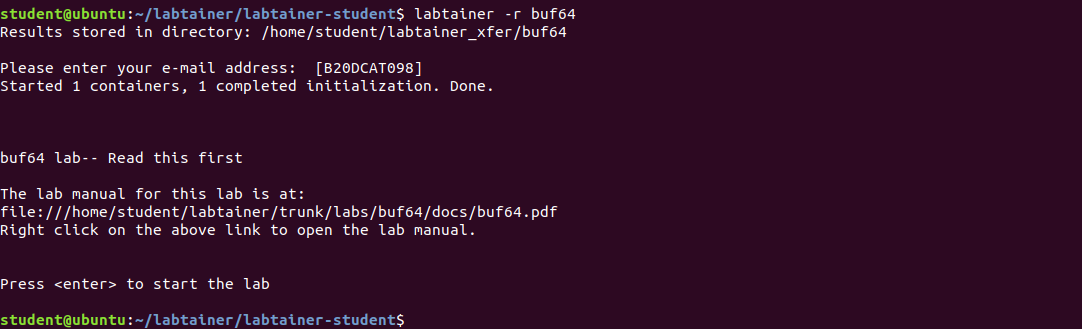
- Sinh viên sử dụng được câu lệnh linux và ngôn ngữ lập trình C.

- Sinh viên đã thực hiện và hiểu bài thực hành Bufoverflow.

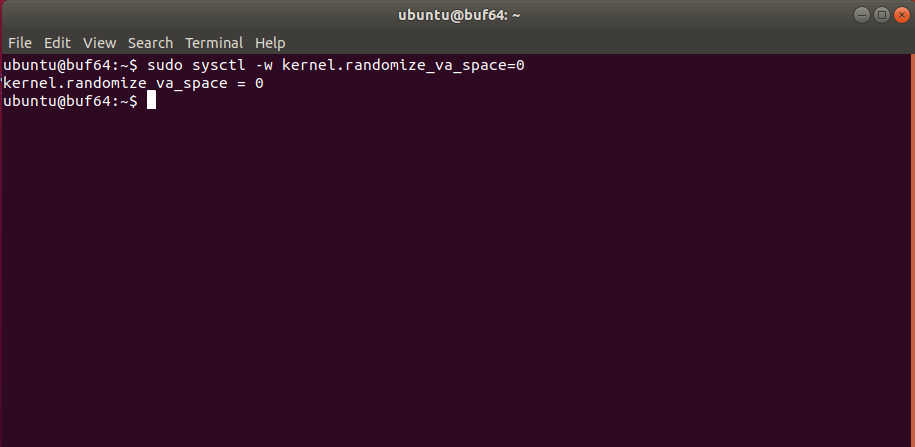
1. **Nội dung thực hành**

Mở terminal, trong thư mục labtainer-student, bắt đầu bài thực hành bằng lệnh:

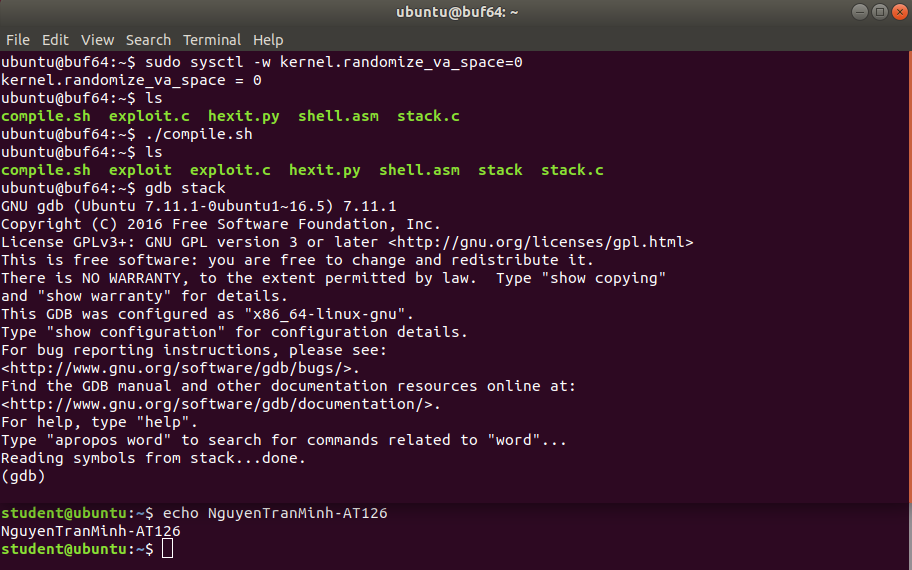
           Labtainer –r buf64



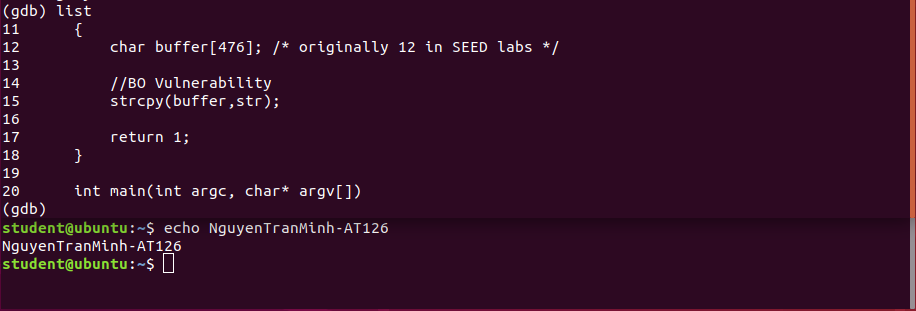
* Vô hiệu hóa ASLR:

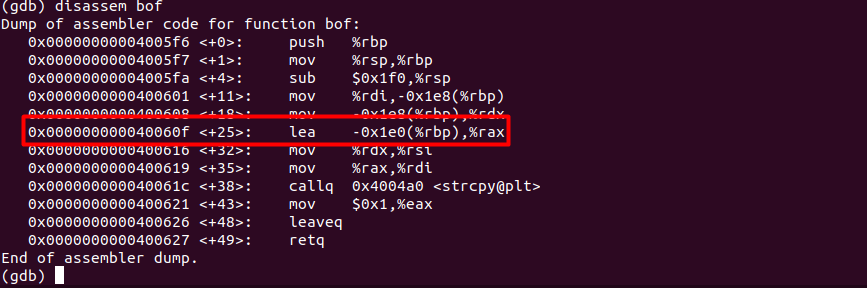


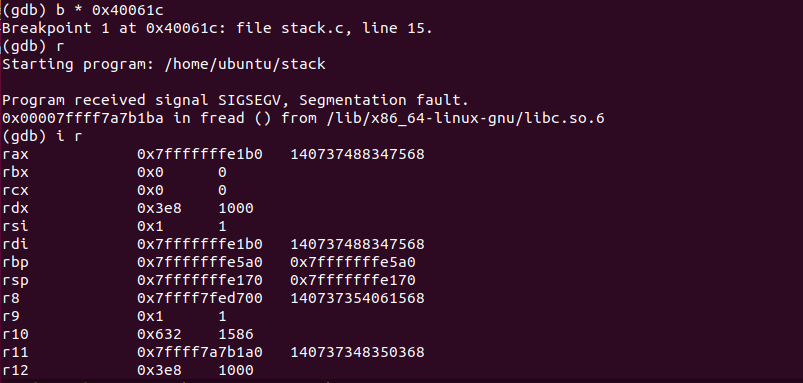
* Chạy compile.sh:



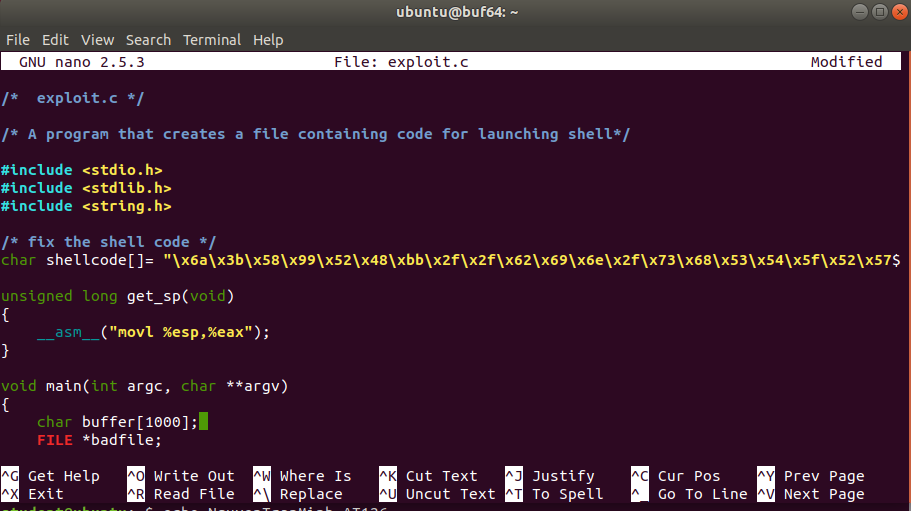
* Sử dụng gdb chạy thử stack:

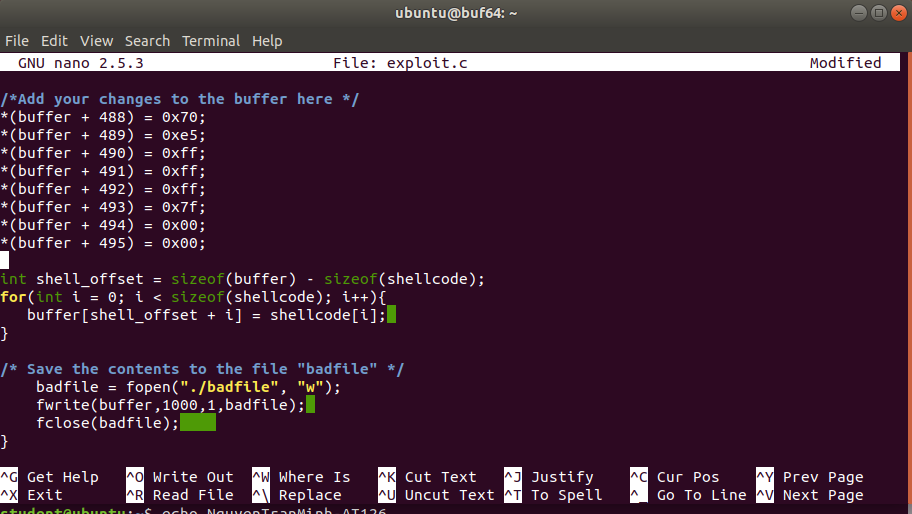




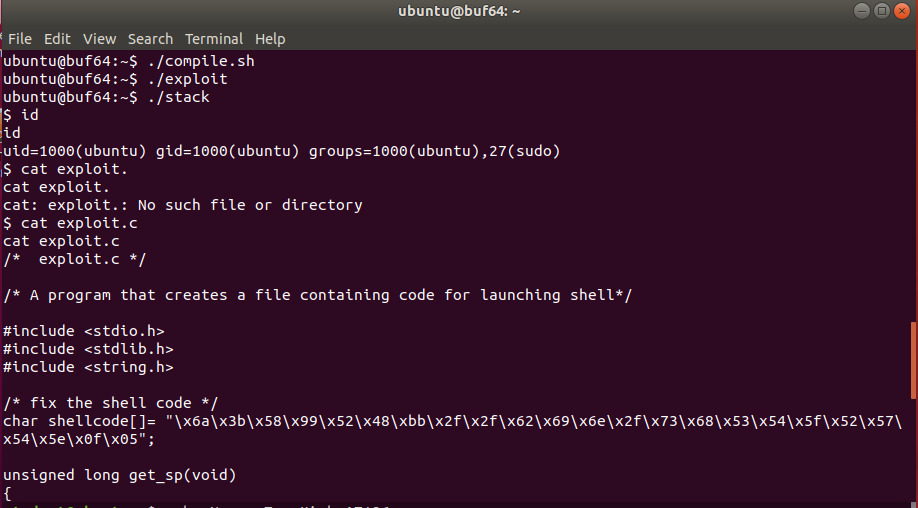


* Shellcode: “\x6a\x3b\x58\x99\x52\x48\xbb\x2f\x2f\x62\x69\x6e\x2f\x73\x68\x53\x54\x5f\x52\x57\x54\x5e\x0f\x05”
* Code tiếp exploit.c:





* Thực hiện khai thác:



# **Checkwork**.

