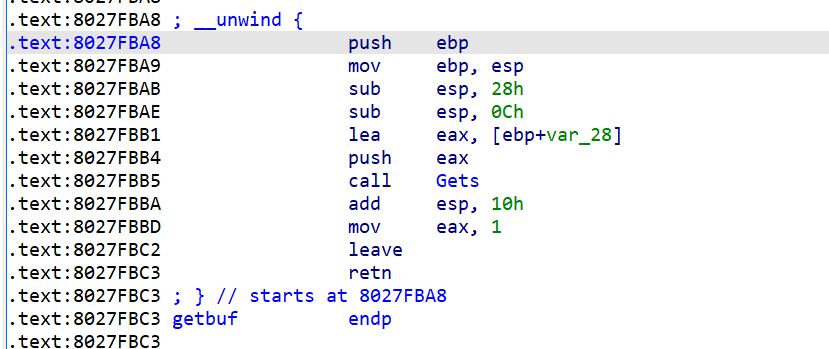
**Báo cáo Lab 5 - Lập trình hệ thống**

Level 0:

- Vẽ stack dựa theo hàm Getbuf bên dưới

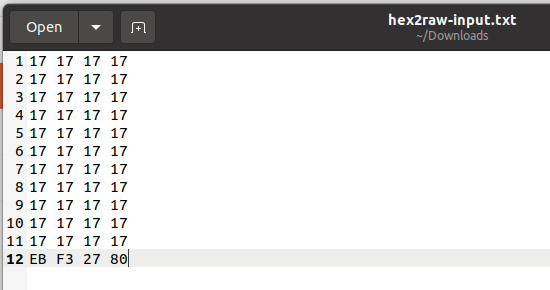
**

*Hình 1: đoạn mã của hàm getbuf*

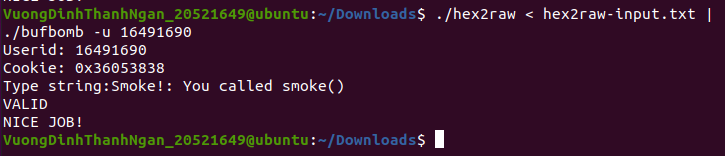
|  |
| --- |
| Return Address |
| ebp |
| Ebp - 40 |
| Ebp - 12 |

- Dựa trên stack trên muốn quay lại vị trí Return add thì cần phải mất 1 khoảng là 44 byte nên ta sẽ nhập vào 44 byte đầu vào. Sau đó để quay lại thì ta sẽ phải nhập thêm 4 byte vị trí của hàm smoke

- Địa chỉ hàm smoke là 8027F3EB viết ngược lại là EBF32780



Hình 2: Chuỗi truyền vào chương trình

**

*Hình 3: Thực thi file bufbomb với chuỗi truyền vào*

Level 1:

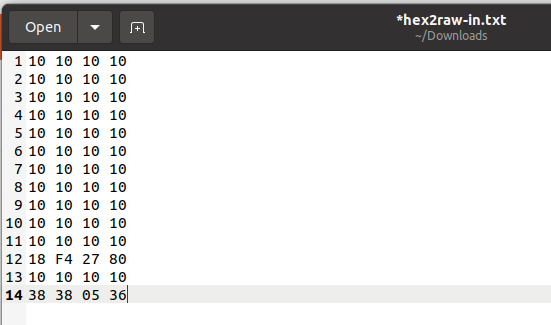
- Ở level này chúng ta có hai stack đó là stack của getbuf và fizz vì chúng ta không thể gọi trực tiếp hàm fizz trong chương trình nên phải thông qua hàm getbuf

- Vẽ Stack:

|  |
| --- |
| Return Address |
| ebp |
| Ebp - 40 |
| Ebp - 12 |

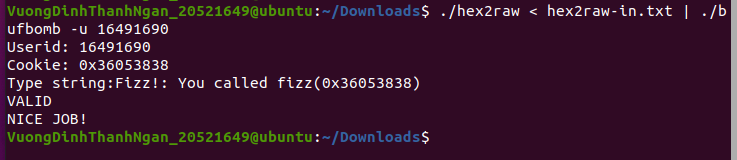
|  |
| --- |
| Return Address |
| ebp |
| Ebp - 8 |
|  |

Getbuf Fizz

**

*Hình 4: Chuỗi truyền vào chương trình*

*-* Chúng ta truyền vào chuỗi tổng cộng là bytes trong đó dòng thứ 12 chính là gì trị địa chỉ của hàm fizz và dòng 14 là giá trị của cookie với phương thức nhập ngược ( cookies 36 05 38 38 => 38 38 05 36)



*Hình 5: Thực hiện chạy file bufbomb*