**Báo cáo lab 6**

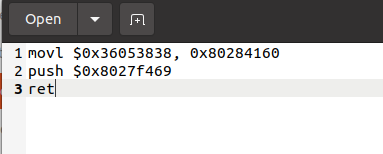
Level 2:

- Thực hiện chạy file bufbomb để xem và debug hàm getbuf

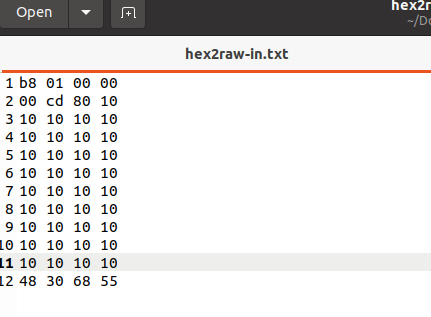
- Stepi 2 lần để tới được hàm hàm push %eax để xem địa chỉ của eax thay đổi như thế nào

- Địa chỉ của eax đã đổi và theo yêu cầu đề bài của level 2 ta phải trở về Cookie của mình từ việc dẫn tới địa chỉ của eax nên ta sẽ build code thực thi chương trình và gán vào file text.

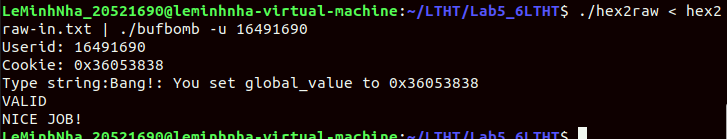
- Khi truyền vào file bufbomb ta cần phải truyền vào 44 giá trị byte hex bất kỳ trong đó các byte hex đầu tiên sẽ là những dòng code thực thi truyền vào. Từ byte thứ 45 là địa chỉ của eax sau khi thay đổi.



*Hình 2.1: Tạo file run chứa đoạn code thực hiện việc kết thúc chương trình*

**

*Hình 2.2: File byte hex được đưa vào chương trình*



*Hình 2.3: Thưc hiệc chạy chương trình thành công*

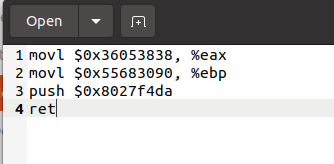
Level 3:

- Ta có Cokkie là: 0x36053838

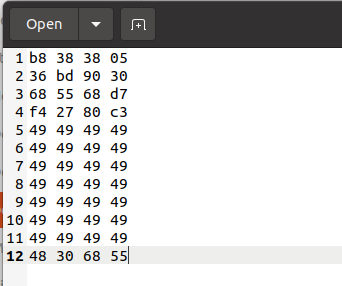
- Thực hiện break lại hàm getbuf ta thấy tại getbuf +12 push %eax. Dùng eax lúc ở getbuf + 12

- Ta lại break tại hàm test và theo dõi địa chỉ của ebp

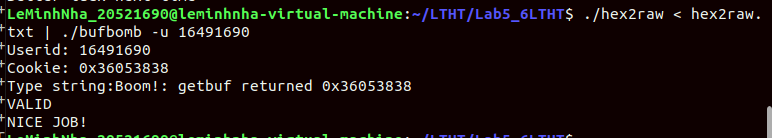
- Ở level 2 vị trí của eax khi thay đổi nên ta cần truyền vào địa chỉ của eax và lưu cookie vào eax, và đẩy vào địa chỉ của hàm uniqueal

**

*Hình 3.1: Tao file chứa đoạn code đưa vào chương trình*



*Hình 3.2: Tạo file chứa cái byte hex đưa vào chương trình*

**

*Hình 3.3: Kết qua chạy chương trình thành công*