

Môn học: Lập trình hệ thống (NT209)

Assignment 5 - Thủ tục/Hàm - Procedure (IA32)

GVHD: Đỗ Thị Thu Hiền

### 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT209.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Phạm Nguyễn Hải Anh	21520586	21520586@gm.uit.edu.vn

## 2. NÔI DUNG THỰC HIÊN:1

STT	Công việc	Kết quả tự đánh giá
1	Câu a	95%
2	Câu b	95%
3	Câu c	95%
4	Câu d	95%
5	Câu e	95%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

 $<sup>^{\</sup>rm 1}$  Ghi nội dung công việc, các kịch bản trong bài Thực hành



# BÁO CÁO CHI TIẾT

Cho đoạn mã assembly như bên dưới.

```
pushl
              %ebp
              %esp, %ebp
3
      movl
      subl
              $40, %esp
              -4(%ebp), %eax
      leal
      movl
              %eax, 8(%esp)
              -8(%ebp), %eax
      leal
              %eax, 4(%esp)
      movl
              $.LCO, (%esp)
      movl
                               Pointer to string "%x %x"
      call
10
              scanf
     Diagram stack frame at this point
      movl
              -4(%ebp), %eax
11
      subl
              -8(%ebp), %eax
12
      leave
13
14
      ret
```

Và đoạn mã C tương ứng:

```
int proc(void)
{
    int a, b;
    scanf("%x %x", &a, &b);
    return b - a;
}
```

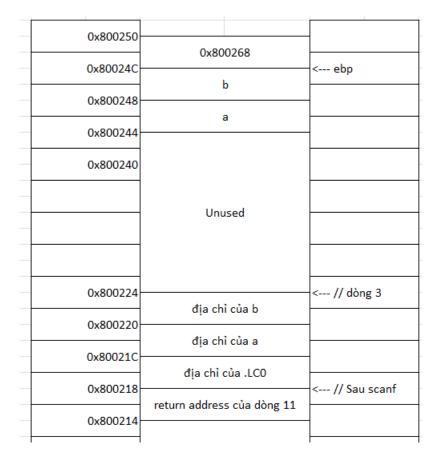
Giả sử khi trước khi thực thi dòng lệnh đầu tiên của **proc** (dòng 1):

%ebp = 0x800268, %esp = 0x800250

- a. Giá trị của %ebp sau dòng lệnh thứ 3 (có giải thích)?
- b. Giá trị của %esp sau dòng lệnh thứ 4 (có giải thích)?
- c. Đoạn code truyền tham số và gọi scanf? Giải thích?
- d. Xác định vị trí cụ thể (địa chỉ) lưu a và b? Giải thích?
- e. Vẽ stack sau khi thực hiện lệnh call scanf.

Lời giải:





a. Giá trị của %ebp sau dòng lệnh thứ 3: 0x80024C vì:

%ebp bắt đầu ở 0x800268. Dòng 2, lưu giá trị hiện tại của %ebp vào stack nên %esp giảm 4, còn lại 0x80024C. Dòng 3, chuyển giá trị của %esp vào %ebp nên giá trị mới của %ebp là 0x80024C.

b. Giá trị của %esp sau dòng lệnh thứ 4: 0x800224 vì:

Giá trị của %esp là 0x80024C trừ đi  $40_{10}$  còn lại 0x800224

c. Đoạn code truyền tham số và gọi scanf là từ dòng 6 tới 10 vì:

Lệnh scanf này cần 3 tham số, 1 cho chuỗi "%x %x" và 2 cho địa chỉ của a, b. Ta thường xác định các dòng truyền tham số bằng lệnh push %<thanh ghi>, bản chất của lệnh này là truyền <thanh ghi> vào stack pointer – 4, tương ứng với câu lệnh movl <thanh ghi>, k(%esp). Ở các dòng 6, 8, 9 ta thấy các dữ liệu được truyền vào 3 ô nhớ liền nhau của %ebp.

d. Địa chỉ lưu a và b lần lượt là: 0x800248 và 0x800244 Vì:

Dòng 4 là dòng cấp phát dữ liệu cho stack nên không liên quan gì a và b.

Dòng 6, 8, 9 theo câu c có mục đích chuẩn bị tham số cho hàm scanf, vậy những biến đó sẽ nằm ở các địa chỉ của thanh ghi đầu tiên của hàm movl. Trong đó, tham số đầu tiên của scanf là "x", di chuyển vào (x", di chuyển vào (x", tham số di chuyển vào 4(x", di chuyển vào (x", di chuyển vào (x", di chuyển vào (x"). Biến a là từ -8(x", b là từ -4(x"), hay .

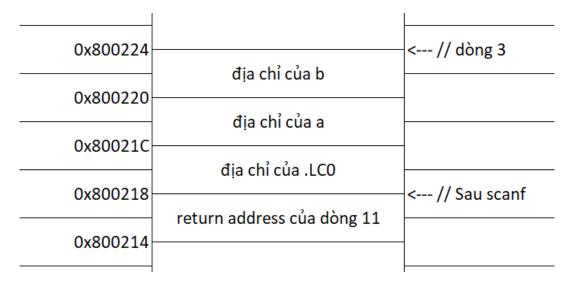
#### **Assignment 04: Machine programming - Procedure**



Logic này càng được khẳng định sau khi thực thi xong hàm scanf, tại dòng 12, %eax = %eax – 8(%ebp), ứng với code là b – a. Vậy 8(%ebp) là a còn 4(%ebp) là b.



e.



Suppose proc calls scanf (line 10), and that scanf reads values 0x46 and 0x53 from the standard input. Assume that the string "%x %x" is stored at memory location 0x300070.

## YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (Report) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

#### Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Đặt tên theo định dạng: [Mã lớp]-AssignmentX\_MSSV.pdf (trong đó X là Thứ tự Assignment, MSSV gồm đầy đủ MSSV của tất cả các thành viên thực hiện bài tập).
   Ví dụ: [NT209.N21.ANTN]-Assignment5\_21520001.pdf.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

#### Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HÉT