

BÁO CÁO LAB 5

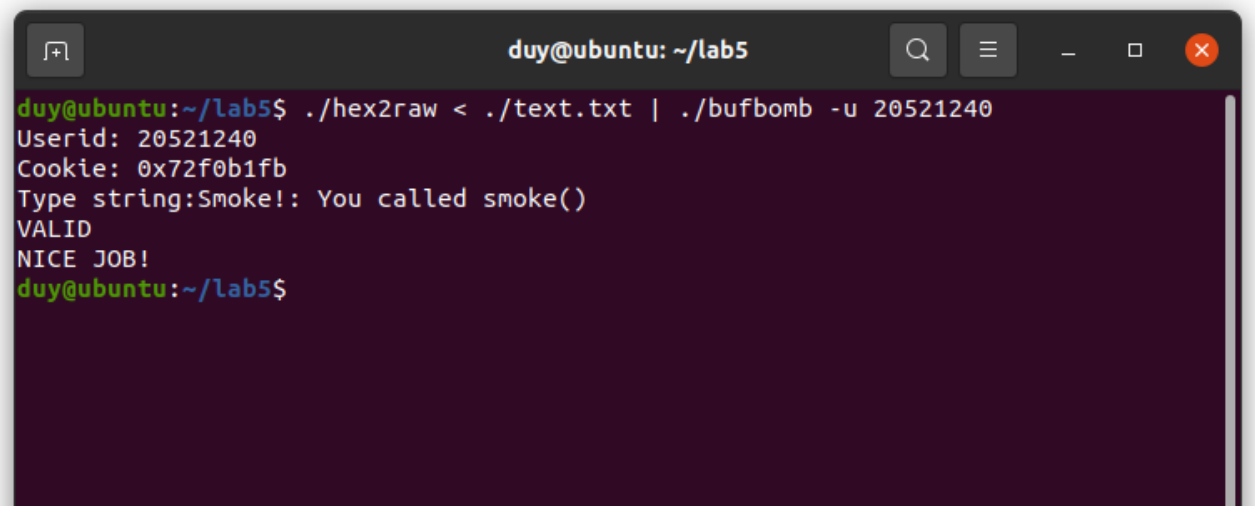
Môn: Lập trình hệ thống

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 <i>(nếu là nhóm)</i>	
Link Video thực hiện <i>(nếu có yêu cầu)</i>	
Ý kiến <i>(nếu có)</i> + <i>Khó khăn gặp phải</i> + <i>Đề xuất, góp ý...</i>	
Điểm tự đánh giá <i>(bắt buộc)</i>	10 /10

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

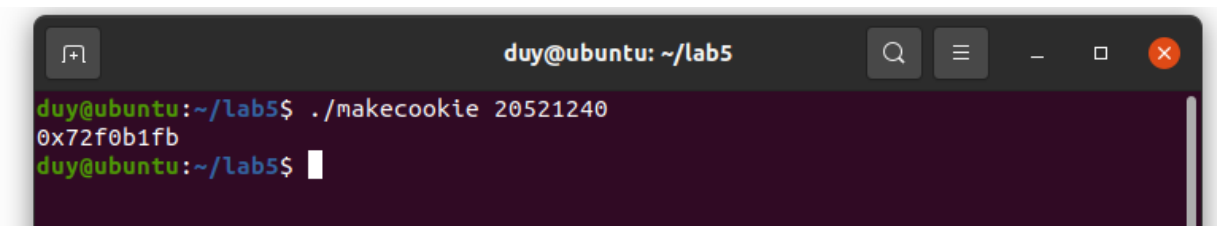
- Ta gõ lệnh `./hex2raw < text.txt | ./bufbomb -u 20521240`



```
duy@ubuntu: ~/lab5
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$
```

Yêu cầu E2.1. Khai thác lỗ hổng 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.



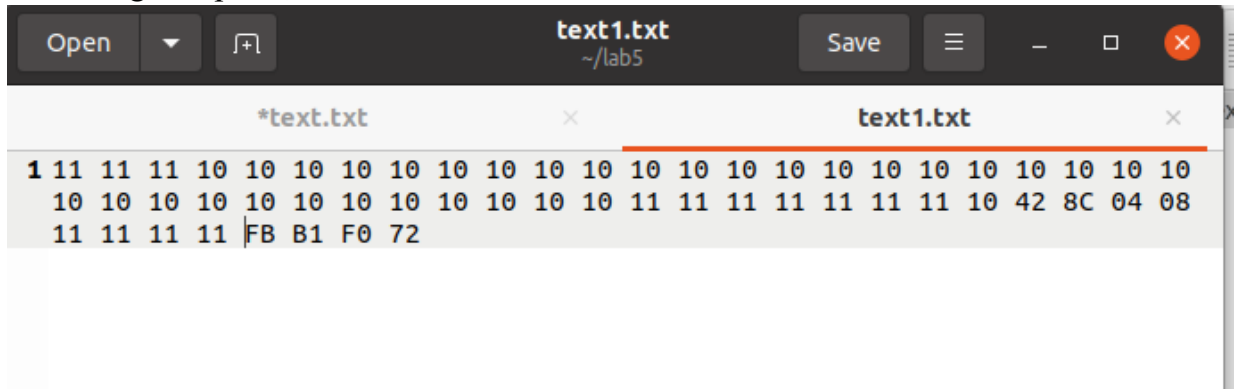
```
duy@ubuntu:~/lab5$ ./makecookie 20521240
0x72f0b1fb
duy@ubuntu:~/lab5$
```

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

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

□ Địa 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”.

