lab 步骤

1. 阅读 bomblab.pdf，了解 lab 需要解决的问题

2. 利用 objdump 反汇编 bomb，阅读各个 phase 的汇编代码

3. 利用 gdb 调试与观察 bomb 程序

4. 观察 phase_1 汇编代码，发现输入值会对比位于 0x402400 的字符串：

```
(gdb) x/s 0x402400
0x402400:       "Border relations with Canada have never been better."
(gdb)
```

得到第一个密文字符串

5. 观察 phase_2 汇编代码，发现调用 read_six_numbers 函数，进一步阅读该函数汇编代码，确定需输入 6 个整数。继续观察 phase_2 汇编代码与利用 gdb 观察相关寄存器数值，发现六个数中，后一个数应为前一个的一倍，测试输入 1，2，4，8，16，32，结果为：

```
gdhnes@gdhnes-Zephyrus-M15-GU502LV-GU502LV:~/csapp-lab$ ./bomb
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
Border relations with Canada have never been better.
Phase 1 defused. How about the next one?
1 2 4 8 16 32
That's number 2.  Keep going!
```

得到第二个密文字符串

6. 观察 phase_3 汇编代码与利用 gdb 观察相关寄存器数值，发现 phase_3 应为 switch-case 结构，选择其中一个 case：

```
400f81: eb 3b                   jmp    400fbe <phase_3+0x7b>
400f83: b8 c3 02 00 00          mov    $0x2c3,%eax
```

测试输出，结果为：

```
gdhnes@gdhnes-Zephyrus-M15-GU502LV-GU502LV:~/csapp-lab$ ./bomb
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
Border relations with Canada have never been better.
Phase 1 defused. How about the next one?
1 2 4 8 16 32
That's number 2.  Keep going!
2 707
Halfway there!
```

得到第三个密文字符串

7. 观察 phase_4 汇编代码与利用 gdb 观察相关寄存器数值，发现 phase_4 需要 2 个输入间存在关系有 ecx = rsi + rax = esi + ((edx -esi) >> 31 + (edx - esi)) / 2 ，综合其他汇编代码内容猜测输入 7，0 可跳出循环，测试输入，结果为：

```
gdhnes@gdhnes-Zephyrus-M15-GU502LV-GU502LV:~/csapp-lab$ ./bomb
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
Border relations with Canada have never been better.
Phase 1 defused. How about the next one?
1 2 4 8 16 32
That's number 2.  Keep going!
2 707
Halfway there!
7 0
So you got that one.  Try this one.
```

得到第四个密文字符串

8. 观察 phase_5 汇编代码与利用 gdb 观察相关寄存器数值，发现 phase_5 需要输入一串字符并与某个字符串对比。类似 phase_1 方法，找到对比的字符串为“flyers”。阅读其他汇编代码，发现输入的字符串将按照某个算法从长串“maduiersnfotvbyl”中转化成另外的串；继续阅读代码，发现按照源字符串中低四位自上面的长串中选取字符，综上推测出源字符串应为“ionefg”，测试输入，结果为：

```
gdhnes@gdhnes-Zephyrus-M15-GU502LV-GU502LV:~/csapp-lab$ ./bomb
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
Border relations with Canada have never been better.
Phase 1 defused. How about the next one?
1 2 4 8 16 32
That's number 2.  Keep going!
2 707
Halfway there!
7 0
So you got that one.  Try this one.
ionefg
Good work!  On to the next...
```

得到第五个密文字符串

9. 观察 phase_5 汇编代码与利用 gdb 观察相关寄存器数值，发现 phase_6 需输入 6 个在 0 与 6 之间的不同数字并与某个序列对比，该序列是由遍历某个链表的值产生的。阅读其他汇编代码，发现该链表会根据输入数字的顺序重排链表；继续阅读代码，发现最终输出要求后一个链节中的值大于本链节中的值，遍历链表，找出各链节的数值，手动重排后，猜测输入数列应为：4 3 2 1 6 5。测试输入，结果为：

```
gdhnes@gdhnes-Zephyrus-M15-GU502LV-GU502LV:~/csapp-lab$ ./bomb
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
Border relations with Canada have never been better.
Phase 1 defused. How about the next one?
1 2 4 8 16 32
That's number 2.  Keep going!
2 707
Halfway there!
7 0
So you got that one.  Try this one.
ionefg
Good work!  On to the next...
4 3 2 1 6 5
Congratulations! You've defused the bomb!
```

得到第六个密文字符串

10.完成实验。