Lab5: Break the Barrier - Experiment Report

学号：PB24061302
姓名：赵国华
院系：人工智能与数据科学学院

1 实验目的

- 理解 strcpy 函数 overflow 的底层原理
- 掌握利用缓冲区溢出进行简单攻击的方法
- 进一步熟悉 trap vectors 和 LC3 工具中的不同模式

2 实验思路

- 编写合适的字符串存入 RO，由 20 个随机字符 + 攻击程序
- 调用 trap x30，触发溢出

3 实验步骤

3.1 将攻击程序写入 R0

使用 LEA 指令将字符串地址加载到 R0，字符串组成：

- 利用.FILL 伪指令填充 20 个随机字符
- 使用汇编语言编写跳转到 x4000 的攻击程序
- 数字 x0000 表示字符串解释

值得注意的点：

- 加载所需的 x4000 地址时使用 LD 指令 + 标签模式，标签也要写到字符串内，否则会出现寻址错误

- 不能使用.STRINGZ 伪指令，否则会在字符串末尾自动添加一个 0，导致攻击程序无法正确执行
- 不能使用.BLKW 伪指令，因为是随机取址，可能会覆盖 x4000 的代码

3.2 触发溢出

使用 TRAP x30 指令触发 strcpy 函数，导致溢出并执行攻击程序。

4 实验结果

成功跳转到 x4000 地址，输出”I make it!”，实验成功。

5 实验总结

通过本次实验，深入理解了 strcpy 函数溢出的原理及其利用方法，掌握了缓冲区溢出攻击的基本技巧，并熟悉了 trap vectors 和 LC3 工具的不同模式操作。发觉自己对于 LEA,LD,LDI 等指令的使用还不够熟练，今后需要多加练习。

测试点信息

#0 通过 / Accepted

本测试点的结果与预期相符。

输入

（无内容）

预期输出

（无内容）

实际输出

```
1  You made it!
```