链接炸弹的 要点提示

对于高版本 的 GCC ,链接时可能会报错。即不区分强、弱符号，只能定义一个符号，另一个符号用引用。可修改 main.c, 将函数指针修改为 extern 说明（此种情况下不能对 main.c 编译链接成一个执行程序）。

实验操作说明

提供的实验包含有 main.c、phase1.o、phase2.o、phase3.o 等。生成执行程序 linkbomb 的方法：

#gcc -c -g main.c -o main.o

#gcc -no-pie -o linkbomb[n] main.o phase[n]*.o n=1、2、3……

例 第二关： gcc -no-pie -o linkbomb2 main.o phase2.o

使用 readelf、hexdump、od、hexedit 等工具阅读和修改目标文件。

另外，实验包中有 phase0.c ，通过该程序，可了解 phase[n].c 的大致写法。

安装 hexedit : apt install hexedit

查看帮助：hexedit -help

最简用法：hexedit filename

在 hexedit 中，F1 ：显示帮助信息； 保存修改结果：F2； 退出不保存：ctrl+c