Bomblab

实验内容

Bomb defuse（70分）：

完成Bomblab主要的实验内容，共计6个phase（60分）以及1个secret phase（10分）。

(选做)完成nuclearlab，学有余力的同学可以尝试。不设置额外分数。

实验报告（30分）：

你的报告需要按照之前的格式，详细解释每一道题的答案以及你的解题思路。如果有需要可以适量配图以及代码。实验报告最后通过githubclassroom提交，具体的详细要求会在之后的作业链接中呈现。

你的爆炸会适当减分，助教会记录你们每个人在第一天之后的爆炸状态。

实验步骤：

1. **下载你的专属bomb💣**

   访问 http://ics.men.ci/bomb，完成微人大验证，点击complie后刷新网页，再点击Download下载你的 bomblab。

   注：短时间访问会导致服务器卡顿，所以有可能刷新后没有反应，属于正常现象。如果长时间无法下载，请联系助教。

2. **布置你的bomb💻**

   今年实验不再限制解答的主机名称，同学们可以在自己的环境下布置（**请使用linux**，其它系统下出现的bug概不负责（bushi））

3. **检查你的bomb🔍**

   ```
   tar -xvf bomblab.tar
   cat README
   ```

   README中有这个炸弹的信息，同学们可以通过对比是否是自己的学号进行判断。每个人的炸弹都是**通过学号定制的**，每个人的答案都不一样，请同学们**不要泄露**自己的bomb。同时也不要把自己的bomb给别人 。

4. **开始拆弹✂️**

   ./bomb中每个炸弹都需要一个输入，当你输入合适的输入后，炸弹就会解除，并视情况进入下一个炸弹。反之，你的炸弹就会爆炸。通过和爆炸都会被记录下来，并上传到服务器。以下是一些拆弹的辅助手段：

   - `objdump` 反汇编： `objdump -d ./bomb > bomb.dump` ， `bomb.dump` 是程序的汇编代码。
   - `gdb` ： `gdb bomb` 。同时在调试时，可以用 `layout asm` 实时查看汇编指令。
   - 你可以将答案记录到一个文件，比如 `solution.txt` ，文件的内容和你拆弹是的输入一致（一行为一个phase的输入）。然后将文件名作为参数启动 `bomb` ，例如 `./bomb solution.txt` ，它会自动读取文件的内容作为输入（如果文件里只写了前几个phase的答案，后续需要在控制台手动输入其它phase的答案）。也可以用gdb启动
   - ```
     gdb -args bomb solution.txt
     ```

5. **我拆掉了吗🔥?**
     ```

通过访问http://ics.men.ci/bomb/scoreboard，可以观察每道题的通过与爆炸情况。数字是爆炸次数，淡青色背景表示题目通过。注意，爆炸次数会一定程度影响你的最终分数（网站分数仅供参考）。ddl之后网站不再接受炸弹的解除信息，请务必在ddl前进行炸弹拆除，并及时关注自己的爆炸情况。

6. **可选nuclear☢**

   拆除nuclearlab会使用到一些常见(?)技巧nuclearlab

   打开参数为：

   - `./nuclearlab <student_id> <password from ics.men.ci/pwd>`
   - 请在http://ics.men.ci/pwd 上获取你的password。
   - 可能需要修改 `nuclearlab` 为可执行 `chmod 755 nuclearlab`

Tips

1. 你需要在 obe 上提交 PDF 版本的实验报告，请确保 scoreboard 上面有你的成绩，实验截至时间初步定在 2024年11月13日晚上23:55。
2. 记得最好在 run/continue 之前确保打好断点，防止爆炸。你也可以思考如何使一个"功能完备"的bomb变得"功能残缺"，使得它无法通信、无法爆炸。这将在某种程度上便利你的拆弹工作。
3. ~~你可以试着不用知道答案，借助gdb速通bomblab（小心栈、变量等各种问题导致程序挂掉）。~~(助教注：现在服务器会在**本地验证**你的代码，也就是说直接跳过去的方式行不通)当然最后你还需要正常完成实验来完成你的报告。
4. 请不要使用过于现代化的工具进行拆弹。你的拆弹过程应当包含理解汇编语言（报告30分）。
5. 如果出现本地拆除、服务端排行榜没同步的情况，在少许等待后如果仍然没反应，请联系助教。
6. 多次拆弹中打断点十分麻烦，可以通过文件设置的方法打断点

   方案一：命令行参数，如 `gdb --ex "break main" program`

   方案二（推荐）：创建.gdbinit文件，并在里面按照以下格式写入断点

   ```
   b phase_1
   b phase_2
   b "想要打断的函数"
   ```

   在使用完之后，记得在gdb运行时输入`info b`查看当前断点状态，防止错误爆炸。
7. 祝大家玩的愉快。

一些出现问题的解决方案

1. 网站还是打不开怎么办

   可以尝试清一下cookies或者重启浏览器。如果以上两者均尝试过但是还是长时间无法登入，请联系助教。

2. 运行中出现 `Password Wrong` 和 `找不到对应路径` 怎么办

   重新生成一下炸弹，这个原因是本地炸弹和服务器信息不匹配造成的。

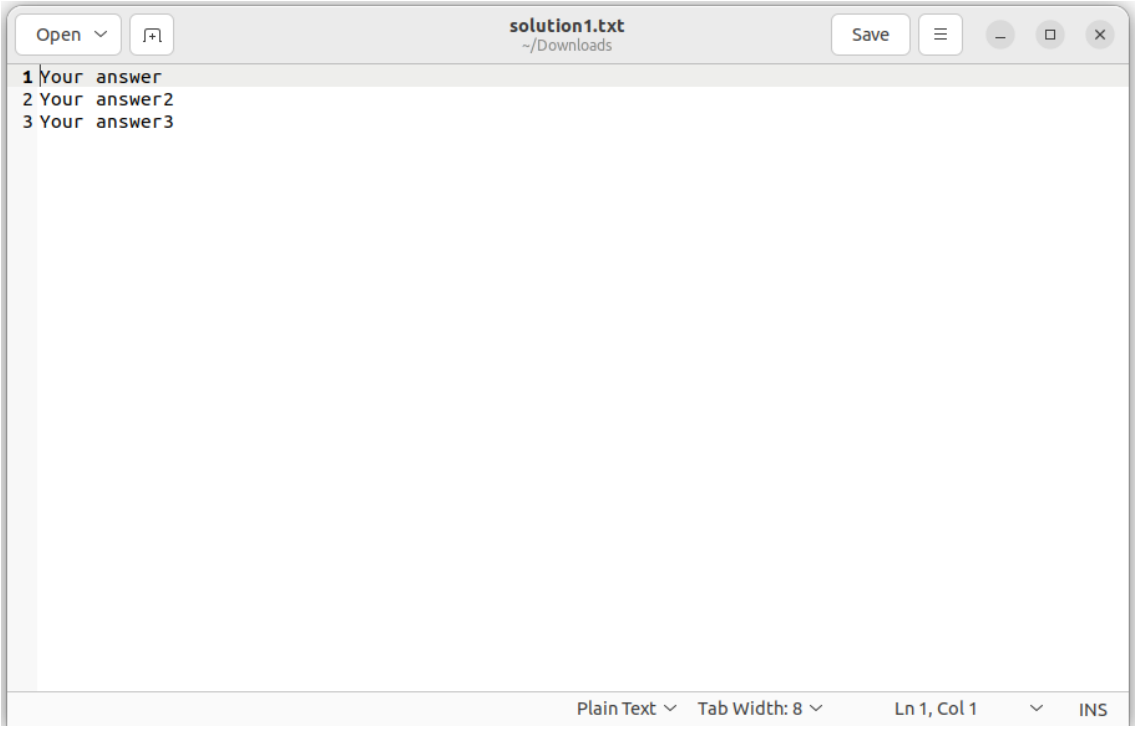
3. 如何将文件放入wsl并解压

   在资源管理器左下方的linux中打开，并按照Ubuntu->home ->用户名的顺序进入，将文件拖进去。随后打开wsl解压即可。

4. 答案正确，但是solution.txt会报错

   这个是因为vscode在保存txt文件时在尾部使用了`CRLF`作为换行符导致的，这个换行符在linux脚本中会引起各种未知bug。

   解决方案：使用`echo "Your answer" >> solution.txt`进行保存，效果如下



5. 权限不足

   输入`chmod 755 bomb`解决问题

6. 在运行中卡在诡异的函数了怎么办

   `CTRL+C`关闭运行程序，随后`quit`退出gdb，之后重新打开就好。