20xx年秋天
实验室任务L2：解除二进制炸弹分配：9月13日，到期：9月22日星期五

哈里·博维克(bovik@cs.cmu.edu)是这个实验室的负责人。

1 导言

邪恶的博士。邪恶在我们的阶级机器上放置了大量的“二元炸弹。 二进制弹是由一系列相组成的程序。 每个阶段都希望您在stdin上键入特定的字符串。 如果键入正确的字符串，则相位被解除，炸弹进入下一个阶段。 否则，炸弹爆炸打印“BOOM！！” 然后终止。 当每一阶段都被拆除时，炸弹就会被拆除。

有太多的炸弹需要我们处理，所以我们给每个学生一个炸弹来拆除。 你别无选择，只能接受的任务是在到期日之前拆除你的炸弹。 祝你好运，欢迎来到拆弹小组！

第一步：拿起你的炸弹

您可以通过将Web浏览器指向：获取炸弹：

```
http://$Bomblab：：SERVER_NAME：$Bomblab：：REQUESTD_PORT/
```

这将显示一个二进制炸弹请求表供您填写。 输入您的用户名和电子邮件地址，然后点击提交按钮。 服务器将在一个名为bombk.tar的tar文件中构建您的bomb并将其返回到浏览器，其中k是您的bomb的唯一编号。

将bombk.tar文件保存到您计划在其中执行工作的（受保护的）目录中。 然后给出命令：tar-xvfbombk.tar。 这将创建一个名为./bombk的目录，其中包含以下文件：

- README：标识炸弹及其所有者。
- 炸弹：可执行的二进制炸弹。

- 来源文件与炸弹的主要常规和友好的问候医生。 邪恶。
- 写作。{pdf，ps}：实验室记录。

如果出于某种原因你要求多个炸弹，这不是问题。 选择一个炸弹来工作，并删除其余的。

第二步：拆除你的炸弹

你在实验室的工作是拆除你的炸弹。

你必须在一个类机器上做作业。 事实上，有传言说博士。 邪恶真的是邪恶，如果跑到别处，炸弹就会爆炸。 还有其他几个防篡改装置也内置在炸弹中，或者说我们听到了。

你可以用很多工具来帮助你拆除炸弹。 请看提示部分，了解一些提示和想法。 最好的方法是使用您最喜欢的调试器来遍历拆卸的二进制文件。

每次你的炸弹爆炸，它都会通知bomblab服务器，你在实验室的最终分数中损失1/2分(最多20分。 所以爆炸的后果是。 你一定要小心！

前四个阶段各值10分。 第5阶段和第6阶段稍微困难一些，所以它们每个值15分。 所以你能得到的最高分数是70分。

虽然阶段逐渐变得更难消除，但当你从阶段转移到阶段时，你所获得的专业知识应该抵消这一困难。 然而，最后一个阶段将挑战即使是最好的学生，所以请不要等到最后一分钟开始。

炸弹忽略空白输入线。 例如，如果你用命令行参数运行炸弹，

```
linux>    。/bomb psol.txt
```

然后，它将从psol.txt读取输入行，直到它到达EOF（文件的末尾），然后切换到stdin。 在虚弱的时刻，博士。 邪恶添加了这个功能，所以你不必继续重新输入解决方案的阶段，你已经排除。

为了避免意外引爆炸弹，您需要学习如何单步通过组装代码和如何设置断点。 您还需要学习如何检查寄存器和内存状态。 做这个实验室的一个很好的副作用是你会非常擅长使用调试器。 这是一项至关重要的技能，它将在你的职业生涯的其余部分带来丰厚的回报。

后勤

这是一个单独的项目。 所有的把手都是电子的。 澄清和更正将张贴在课程留言板上。

手把手

没有明确的交接。 炸弹将自动通知你的教练你的进展，因为你的工作。 你可以通过查看课堂记分板来跟踪你的表现：

http://$Bomblab：：SERVER_NAME：$Bomblab：：REQUESTD_PORT/scoreboard

此网页不断更新，以显示每个炸弹的进度。

提示(请读这个！)

拆除你的炸弹有很多方法。 您可以非常详细地检查它，而不必运行程序，并准确地了解它的作用。 这是一种有用的技术，但并不总是容易做到。 您还可以在调试器下运行它，一步一步地观察它所做的事情，并使用这些信息来消除它。 这可能是最快的方法来化解它。

我们确实提出了一个要求，请不要使用暴力！ 你可以写一个程序，尝试每一个可能的键，以找到正确的。 但这有几个原因：

- 每次你猜错，炸弹爆炸，你就会损失1/2分(最多20分。
- 每次你猜错了，都会向bomblab服务器发送一条消息。 您可以非常快地用这些消息使网络饱和，并导致系统管理员撤销您的计算机访问。
- 我们没有告诉你字符串有多长，也没有告诉你字符串中的字符。 即使你做了（不正确的）假设，它们都小于80个字符长，并且只包含字母，那么你将有26^{80} 每个阶段的猜测。 这将需要很长的时间来运行，您将无法在作业到期前得到答案。

有许多工具被设计来帮助你找出程序是如何工作的，以及当它们不工作时什么是错误的。 这里列出了一些在分析炸弹时可能有用的工具，并提示如何使用它们。

- gdb

  GNU调试器，这是一个几乎每个平台都可用的命令行调试器工具。 您可以逐行跟踪程序，检查内存和寄存器，同时查看源代码和程序集代码（我们没有为您的大部分炸弹提供源代码），设置断点，设置内存监视点，并编写脚本。

  CS：APP网站

  http://csapp.cs.cmu.edu/public/students.html

  有一个非常方便的单页gdb摘要，您可以打印出来并用作参考。 以下是使用gdb的一些其他技巧。

- 为了防止每次输入错误时炸弹爆炸，您需要学习如何设置断点。
- 对于在线文档，在gdb命令提示符下键入“帮助”，或在Unix提示符下键入“man gdb”或“info gdb。 有些人也喜欢在emacs中的gdb模式下运行gdb。

- objdump-t

  这将打印出炸弹的符号表。 符号表包括炸弹中所有函数和全局变量的名称、炸弹调用的所有函数的名称及其地址。 您可以通过查看函数名了解一些东西！

- objdump-d

  用这个来拆卸炸弹中的所有代码。 您也可以只查看单个函数。 阅读汇编程序代码可以告诉你炸弹是如何工作的。

  虽然objdump-d给了你很多信息，但它并没有告诉你整个故事。 对系统级函数的调用以神秘的形式显示。 例如，对sscanf的调用可能显示为：

  8048c36：e899fcff调用80488d4<_init+0x1a0>

  要确定调用的是sscanf，您需要在gdb中拆卸。

- 弦

  此实用程序将显示炸弹中的可打印字符串。

寻找特定的工具？ 文件怎么样？ 别忘了，命令和信息是你的朋友。 特别是，人类ascii可能会有用。 信息气体将给你比你想知道的GNU汇编程序更多。 此外，网络也可能是一个信息宝库。 如果你遇到困难，请随时向你的导师寻求帮助。