15 - 213 下跌 20
XX

实验作业 L2:拆除一枚双体炸弹分配日期:9 月 13 日，截止日期:9 月 22 日(星期五)

Harry Bovik (bovik@cs.cmu.edu)是这个实验室的负责人。

1 介绍

邪恶的 Dr. Evil 在我们的班级机器上安装了大量的“二进制炸弹”。“二元炸弹”是一个由一系列阶段组成的程序。每个阶段都希望你在 stdin 上输入一个特定的字符串。如果你输入正确的字符串，那么该阶段被解除，炸弹继续进入下一个阶段。否则，炸弹会通过打印“BOOM!!”然后终止而爆炸。当每个阶段都被拆除时，炸弹就被拆除了。

我们要处理的炸弹太多了，所以我们给每个学生一个炸弹去拆除。你们不得不接受的任务，就是在截止日期之前拆除炸弹。祝你好运，欢迎加入拆弹小组!

第一步:带上炸弹

你可以通过打开浏览器来获取你的炸弹:

http:// Bomblab:美元:SERVER_NAME: $ Bomblab:: REQUESTD_PORT /

这将显示一个二进制炸弹请求表单，供您填写。输入你的用户名和电子邮件地址，然后点击提交按钮。服务器将构建你的炸弹，并以名为 bombk 的 tar 文件返回给你的浏览器。Tar，其中 k 是你的炸弹的唯一编号。

将 bombk.tar 文件保存到你计划在其中工作的(受保护的)目录中。然后输入命令:tar -xvf bombk.tar。这将创建一个名为./bombk 的目录，其中包含以下文件:

- README:识别炸弹及其所有者。

bomb:可执行二进制炸弹。

•炸弹。c:带有炸弹的主要程序和邪恶博士友好问候的源文件。

•那样。{pdf,ps}:实验写作。

如果出于某种原因你要求多枚炸弹，这不是问题。选择一个炸弹进行处理，然后删除其余的。

第二步:拆除炸弹

你在这个实验室的工作是拆除炸弹。

你必须在其中一台机器上完成作业。其实有传言说，邪恶博士真的很邪恶，如果跑到别的地方，炸弹总是会爆炸。炸弹里还内置了其他几个防篡改装置，至少我们是这么听说的。

你可以使用许多工具来帮助你拆除炸弹。请查看提示部分获取一些提示和想法。最好的方法是用你最喜欢的调试器单步调试反汇编的二进制文件。

每次你的炸弹爆炸，它都会通知炸弹服务器，你会在实验室的最终得分中损失 1/2 分(最多 20 分)。所以炸弹爆炸是有后果的。你一定要小心!前四个阶段各 10 分。第五阶段和第六阶段难度要大一些，所以每个阶段值 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化解，但你从一个阶段移动到另一个阶段所获得的专业技能应该可以抵消这个难度。然而，最后一个阶段甚至会挑战最优秀的学生，所以请不要等到最后一分钟才开始。

炸弹会忽略空白的输入行。例如，如果你使用命令行参数运行炸弹，

```
linux > psol.txt /炸弹
```

然后它会从 psol.txt 读取输入行，直到到达 EOF (file end of)，然后切换到 stdin。邪恶博士在一时无力的时候加入了这个功能，这样你就不用一直重复输入你已经化解的阶段的解决方案了。

为了避免意外引爆炸弹，你需要学习如何单步通过汇编代码，以及如何设置断点。你还需要学习如何检查寄存器和内存状态。做实验的一个好处是，你会非常擅长使用调试器。这是一项至关重要的技能，将为你的职业生涯带来巨大的回报。

物流

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

Handin

没有明确的 handin。炸弹会在你练习的时候自动通知你的导师你的进度。你可以通过查看课程记分牌来了解自己的学习情况:

http:// Bomblab 美元::SERVER_NAME: $ Bomblab:: REQUESTD_PORT /记分板

本网页会不断更新，以显示每枚炸弹的进展情况。

提示(请阅读此处!)

解除炸弹的方法有很多。你可以在不运行程序的情况下详细地检查它，并弄清楚它到底做了什么。这是一项有用的技术，但并不总是容易做到。你也可以在调试器下运行它，一步一步观察它的表现，然后利用这些信息去化解它。这可能是化解它最快的方法了。

我们有一个要求，请不要使用暴力!你可以写一个程序，尝试每一个可能的密钥来找到正确的。但这样做是不行的，原因如下。

- 每次你猜错，炸弹爆炸，你会失去 1/2 分(最多 20 分)。
- 每猜错一次，炸弹服务器就会收到一条消息。你可能很快就会被这些消息充斥网络，导致系统管理员取消你的计算机访问权限。
- 我们没有告诉你这些字符串有多长，也没有告诉你它们包含哪些字符。即使你(不正确地)假设它们的长度都小于 80 个字符，并且只包含字母，那么你将得到 26 个字符 ^{80} 对每个阶段进行猜测。这将花费很长时间，并且在作业到期前你不会得到答案。

有许多工具被设计来帮助你弄清楚程序是如何工作的，以及当它们不起作用时是什么问题。下面是一些工具的列表，你可能会发现有用的分析你的炸弹，并提示如何使用它们。

- gdb

  GNU 调试器，这是一个命令行调试工具，几乎在每个平台上都可以使用。你可以逐行跟踪一个程序，检查内存和寄存器，同时查看源代码和汇编代码(我们不会给你大部分炸弹的源代码)，设置断点，设置内存观察点，以及编写脚本。

  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，你可以打印出来作为参考。这里还有一些使用 gdb 的技巧。

-为了避免每次输入错误时炸弹就爆炸，你需要学习如何设置断点。

-对于在线文档，在 gdb 命令提示符下输入“ help”，或者在 Unix 提示符下输入“ man gdb”，或者“info gdb”。有些人也喜欢在 emacs 中以 gdb 模式运行 gdb。

- objdump -t

  这会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，以及它们的地址。通过查看函数名，你可能会学到一些东西!

- objdump -d

  使用它来反汇编炸弹中的所有代码。你也可以只查看单个函数。阅读汇编代码可以告诉你炸弹是如何工作的。

  虽然 objdump -d 能给你很多信息，但它并不能告诉你整个故事。对系统级函数的调用以一种神秘的形式显示出来。例如，对 sscanf 的调用可能显示为:

```
8048        E8 99 fc ff ff    调      80488 d4 < _init + 0
```

  要确定调用是对 sscanf 的，需要在 gdb 内部进行拆解。

- 字符串

  这个实用程序将显示炸弹中的可打印字符串。

寻找特定的工具?文档怎么样?别忘了，命令 apropos、man 和 info 是你的朋友。特别地，man ascii 码可能会有用。info gas 将为您提供更多关于 GNU 汇编程序的信息。此外，网络也可能是一个信息的宝库。如果你被难住了，请随时向你的老师寻求帮助。