15-213 秋季 20xx

实验室作业 L2:拆除二元炸弹 分配时间:9 月 13 日,截止日期:9 月 22 日星期五

Harry Bovik (bovik@cs.cmu.edu) 是该实验室的负责人。

1 简介

邪恶的Dr. Evil在我们班级的机器上安放了一系列“二进制炸弹”。二进制炸弹是一个由一系列阶段组成的程序。每个阶段都希望您在标准输入中键入一个特定的字符串。
如果您键入正确的字符串,则该阶段将被拆除,炸弹将进入下一阶段。否则,炸弹通过打印“BOOM!!!”爆炸。然后终止。当每个阶段都被拆除时,炸弹就会被拆除。

炸弹太多我们无法处理,所以我们给每个学生一个炸弹来化解。你的任务,你别无选择,只能接受,就是在截止日期前拆除你的炸弹。祝你好运,欢迎来到拆弹小队!

第 1 步:获取炸弹

您可以通过将 Web 浏览器指向以下位置来获取炸弹:

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

这将显示一个二进制炸弹申请表供您填写。输入您的用户名和电子邮件地址,然后点击提交按钮。服务器将构建您的炸弹并将其通过名为 bombk.tar 的 tar 文件返回给您的浏览器,其中 k 是您的炸弹的唯一编号。

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

- 自述文件:识别炸弹及其所有者。
- 炸弹:可执行二进制炸弹。

- bomb.c:包含炸弹主要例程和邪恶博士友好问候的源文件。
- writeup.{pdf,ps}:实验室文章。

如果出于某种原因您请求多个炸弹,这不是问题。选择一个炸弹进行处理并删除其余的。

第 2 步:拆除炸弹

你在这个实验室的工作是拆除你的炸弹。

您必须在其中一台课堂机器上完成作业。事实上,有传言说邪恶博士真的很邪恶,跑到别处炸弹总会爆炸。炸弹中还内置了其他几种防篡改装置,至少我们是这么听说的。

您可以使用许多工具来帮助您拆除炸弹。请查看提示部分以获得一些提示和想法。最好的方法是使用您最喜欢的调试器逐步执行反汇编的二进制文件。

每次你的炸弹爆炸时,它都会通知炸弹实验室服务器,你会在实验室的最终分数中失去 1/2 分(最多 20 分)。所以引爆炸弹是有后果的。你一定要小心!

前四个阶段各得 10 分。第 5 阶段和第 6 阶段稍微困难一些,因此每个阶段都值 15 分。所以你能得到的最高分是70分。

尽管阶段变得越来越难以化解,但您从一个阶段移动到另一个阶段时获得的专业知识应该可以抵消这种困难。然而,最后阶段即使是最优秀的学生也会面临挑战,所以请不要等到最后一刻才开始。

炸弹忽略空白输入行。例如,如果您使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,直到到达 EOF(文件末尾),然后切换到标准输入。在虚弱的时刻,Evil 博士添加了此功能,这样您就不必不断地重新输入解决方案来解决您已经解决的问题。

为避免意外引爆炸弹,您需要学习如何单步执行汇编代码以及如何设置断点。您还需要学习如何检查寄存器和内存状态。完成该实验室的一个好处是您将非常擅长使用调试器。这是一项至关重要的技能,它将为您的余下职业生涯带来丰厚回报。

后勤

这是一个单独的项目。所有的递交都是电子的。澄清和更正将张贴在课程留言板上。

带来

没有明确的递交。炸弹会在您处理它时自动通知您的讲师您的进度。您可以通过查看班级记分牌来跟踪您的表现：

http://$Bomblab::SERVER_NAME:$Bomblab::REQUESTD_PORT/记分牌

该网页不断更新，以显示每个炸弹的进度。

提示（请阅读此内容！）

有很多方法可以拆除你的炸弹。您可以在不运行程序的情况下详细检查它，并弄清楚它的作用。这是一项有用的技术，但并不总是那么容易做到。您还可以在调试器下运行它，逐步观察它的作用，并使用此信息来化解它。这可能是化解它的最快方法。

我们提出一个要求，请不要使用暴力！您可以编写一个程序，尝试使用所有可能的密钥来找到正确的密钥。但由于以下几个原因，这并不好：

- 每次您猜错并且炸弹爆炸时，您将失去 1/2 分（最多 20 分）。
- 每次您猜错时，都会向炸弹实验室服务器发送一条消息。您可能会很快使网络充满这些消息，并导致系统管理员撤销您的计算机访问权限。
- 我们没有告诉您字符串有多长，也没有告诉您其中有哪些字符。即使您做出（不正确的）假设，即它们的长度都少于 80 个字符并且仅包含字母，那么每个阶段您都会有2680 次猜测。这将需要很长时间才能运行，并且您不会在作业到期之前得到答案。

有许多工具旨在帮助您了解程序如何工作，以及当它们不工作时出了什么问题。这里列出了一些您可能会发现对分析炸弹有用的工具，以及如何使用它们的提示。

- gdb

  GNU 调试器，这是一个几乎在每个平台上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，同时查看源代码和汇编代码（我们不会为您提供大部分炸弹的源代码），设置断点，设置内存观察点，然后编写脚本。

  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。

–对于联机文档,在 gdb 命令提示符下键入“help”,或在 Unix 提示符下键入“man gdb”或“info gdb”。有些人还喜欢在 gdb-mode 下运行 gdb
emacs。

- 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。你可以通过查看函数名称来学习一些东西!

- objdump -d

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

  尽管 objdump -d 为您提供了很多信息,但它并没有告诉您全部情况。对系统级函数的调用以神秘的形式显示。例如,可能会出现对 sscanf 的调用
  作为:

  8048c36: e8 99 fc ff ff 调用 80488d4 <_init+0x1a0>

  要确定调用的是 sscanf,您需要在 gdb 中进行反汇编。

- 字符串

  该实用程序将显示炸弹中的可打印字符串。

寻找特定工具?文档怎么样?不要忘记,命令 apropos、man 和 info 是您的朋友。特别是,man ascii 可能会派上用场。 info gas 会给你比你想知道的更多关于 GNU 汇编程序的信息。此外,网络也可能是信息的宝库。如果您遇到困难,请随时向您的导师寻求帮助。