BombLab 指导 - 2022

实验内容

- ***Bomb Defusion***

完成`bomblab`，**共6 phases和1个secret phase**。

【可选】完成`nuclearlab`**（不额外加分）**。

- **实验报告**

说明实验过程。包括但不限于每个phase的解决方法、理解思路，可以适当配图或代码辅助说明。报告不做严格格式要求，但请保证语言正确、简洁，**不鼓励长篇大论**。

实验步骤（以`bomblab`为例）

1. **下载你的专属bomb💣**

访问https://ics.men.ci/bomb，完成微人大认证，点击compile并刷新，在显示下载字样后下载`bomblab`。

⚠️请注意，为了方便自动统计同学们的成绩，每个bomb内都包含对应同学的验证信息，请确保你拆除的是自己下载的bomb！

2. **将bomb上传或拷贝到合适的Linux平台上💻**

上传`bomblab.tar`到你在`ics.ruc.rvalue.moe`的账户中。这里我们使用`scp`方法：

```
scp <bomb_local_path> <username>@ics.ruc.rvalue.moe:<bomb_remote_path>
```

例如，`scp Desktop/bomblab.tar 2021000000@ics.ruc.rvalue.moe:~`表示将本地`Desktop`中的bomb上传至服务器里的用户目录中。

3. **检查你的bomb🔍**

请根据你的目录和系统环境执行下面的命令。

```
ssh <username>@ics.ruc.rvalue.moe
cd <bomb_upload_directory_path>
tar -xvf <bomb_tar_path>
ls
cd bomblab
cat README
```

⚠️请注意，`README`中的内容需要是你的信息。否则请重新下载或联系助教。

你的`bomblab`文件夹的目录树应该是这样的：

```
.
├── README   # 你的个人信息
├── bomb     # 你的专属bomb
└── bomb.c   # 供参考的bomb框架
```

4. **开始拆弹✂️**

依次阅读bomb的内容，并尝试对每个`phase`给出要求的输入，然后你将得到对应的反馈。**如果答案错误炸弹就会爆炸！**每个`phase`的每次尝试都会发送信息给服务器记录你成功与否。

你可以使用下面的方法辅助你得到结果：

- `objdump`反汇编：`objdump -D -S ./bomb > bomb.dump`
- `gdb`调试：`gdb ./bomb`
- 瞪眼看、瞎猜等**创新性解法**

5. **爆炸了吗💥**

如果你的某次尝试不幸失败，一个“功能完备”的bomb将和服务器通信，并记录你的这次“死亡”。**每次爆炸都可能或多或少地影响你的最终分数。**

⚠️请注意：

- 一个“功能完备”的bomb每次尝试拆除时都会和服务器通信，以确保能够向服务器发送你的拆除结果。如果在检查通信时发现无法通信，拆弹程序将自动终止。所以，你可能无法在本地平台成功运行一个“功能完备”的bomb。
- 请保护好自己的bomb不要落入“坏人”手中。上传至服务器时请确保它在你的个人文件夹内。每次爆炸都是不可逆的。

6. **可选nuclear☢️**

拆除nuclearlab会使用到一些常见**(?)**技巧，~~因为过于常见这里不再赘述~~。

nuclearlab的打开参数为：`./nuclearlab <student_id> <password from ics.men.ci/pwd>`。

提交

你需要且仅需要在`obe`上提交***PDF***版本的实验报告，并确保`ics.men.ci`上有你的成绩。

实验截止时间初步定在**2022年11月11日晚上23:55**。

Tips

1. 你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。
2. 本次实验过程中，助教原则上不会在有关工具的使用上给出技术性指导，希望同学们自行查阅资料，培养独立解决问题的能力。**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。**
3. 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**，否则可能会很大地影响助教的心情。
4. **祝大家炸的绚烂！**

参考资料

[0] 微信群中的共享文档

[1] CMU BombLab 指导`Defusing a Binary Bomb.pdf`

[2] `Bomb实验相关内容.pptx`

[3] GDB调试指南 https://www.yanbinghu.com/2019/04/20/41283.html

[4] ICS I 课程材料