Attacklab 实验说明 2021

1 实验要求和内容

- 可执行文件 `ctarget` 和 `rtarget` 是本次实验的题目文件，其中共包含五道题目
  - `ctarget` 的3道题为代码注入攻击，`rtarget` 的两道题为ROP攻击
- 需要在Linux环境下使用GDB调试、反汇编等方法来完成此次实验
- 实验报告需要详细写出求解密码的过程（但不鼓励篇幅过长）

2 实验步骤

2.1 登录服务器

- 服务器地址：`202.112.113.122` 或 `ics.ayaya.in`
- 用户名和密码与前两次实验相同

2.2 下载文件

- 在服务器上打开终端，输入以下命令：

  ```
  wget -O a.tar "localhost:8020/?username=你的学号&usermail=你的学号%40qwq.com&submit=Submit"
  ```

  将标识为"你的学号"的地方使用学号代替。该命令会下载一个名为 `a.tar` 的文件到终端当前的路径里，可以使用 `pwd` 查看当前路径。

- 解压缩

  ```
  tar xvf a.tar
  ```

  此时会解压出一个名为 `targetN` 的目录，`N` 是一个数字编号。该目录包含了本实验所需的文件。

2.3 反汇编

- 查看解压后的文件
  - `ctarget`：可执行程序，要完成三次代码注入攻击
  - `rtarget`：可执行程序，要完成两次ROP攻击
  - `cookie.txt`：用于验证身份，无需修改
  - `farm.c`：用于产生ROP攻击（代码源）
  - `hex2raw`：将你的攻击文本转换为生字符串的工具
- 反汇编
  - `objdump -d ./ctarget > asm1`
  - 你可以在 `asm1` 文件中找到 `ctarget` 的反汇编代码

2.4 阅读材料

请务必在实验前认真阅读本文件以及 `attacklab.pdf`。后者是原始包中的详细实验介绍，读完之后，你将会对本次实验的流程有一个较全面的了解。

2.5 尝试攻击

- 仔细观察反汇编代码，给出对于每个题目的攻击代码
- 将攻击代码写入文本文件（例如 `ans1.txt` ），每两个十六进制位之间需要添加空格
- 进行攻击。攻击时，你需要使用 `hex2raw` 将你的文本文件转换为生字符串，作为 `target` 的输入

```
cat ans1.txt | ./hex2raw | ./ctarget
```

- 如果成功，会有提示信息，结果自动上传至服务器。失败没有代价。

2.6 分数与提交

- 查看得分：`http://ics.ayaya.in:8020/scoreboard`
- 请把你认为必要的东西写入实验报告（例如完成度、攻击串、攻击的详细过程或思路等）
- 祝大家实验愉快！
- 提交内容包括实验报告、下载的 `a.tar` 压缩包、五道题对应的攻击串文件。提交的压缩包命名为 `学号-attacklab.zip`，压缩包内文件请按如下规则命名：
  - 实验报告：实验报告.pdf
  - `a.tar` 压缩包：`a.tar`
  - 攻击串文件按题目顺序依次命名为：`1.txt` `2.txt` `3.txt` `4.txt` `5.txt`

  在 OBE 上提交的压缩包内部不要包含子文件夹。