Attack Lab 指导 2022

实验内容和要求

1.可执行文件ctarget和rtarget，包括5道密码（3道代码注入攻击 + 2道ROP攻击）

2.方法：反汇编、GDB调试（Linux环境）

3.实验报告：详细求解密码的过程（但不鼓励篇幅过长）

实验步骤

1.下载$target$

首先登陆服务器，同之前的Lab一样

```
ssh <你的学号>@ics.ruc.rvalue.moe
```

然后下载$attack.tar$

```
wget -O attack.tar "localhost:15513/?username=你的学号&usermail=你的学号%40ruc.edu.cn&submit=Submit"
```

将标识为“你的学号”的地方用学号代替。该命令会下载一个名为$attack.tar$的文件到你当前的路径下，可以使用pwd查看当前路径。

2.解压缩

此时会解压出一个$target N$的目录，N仅仅是一个数字编号

```
tar xvf attack.tar
```

3. 反汇编

查看解压后的文件

- ctarget： 可执行程序，要完成3次代码注入攻击
- rtarget：可执行程序，要完成2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）
- hew2raw：一个生成攻击字符串的工具

```
objdump -d ./ctarget > asm
```

- 你可以在asm文件种找到ctarget的反汇编代码

提示：可以传回本地看更方便

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。

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，你需要使用到如下命令

```
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。

6. 分数与提交

- 查看得分：http://ics.ruc.rvalue.moe:15513/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，你的$attacklab.tar$，以及下载的五道题对应的攻击串文件（请分别命名为$1.txt$，$2.txt$，$3.txt$，$4.txt$，$5.txt$）。