Attacklab 实验说明 2019

1 实验内容和要求

- 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）
- 方法：反汇编、GDB 调试（Linux 环境）
- 实验报告：详细求解密码的过程

2 实验步骤

2.1 下载 target

- [http://192.144.238.229:15513]
- 用户名为服务器上的用户名，填写自己的 email
- 会下载一个随机生成的 targetN 压缩包

2.2 登录 Linux 服务器

- 服务器 IP：192.144.238.229
- 用户名和密码同前两次实验
- 上传自己的 `targetN.tar`
- 登录服务器，输入 `tar -xvf ./targetN.tar` 命令解压缩

> 请不要在 Windows 上解压 `targetN.tar` 再上传服务器，会导致文件损坏。

2.3 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
- 反汇编

```
objdump -d ./ctarget > asm1
```

- 可以传回本地看更方面

2.4 阅读材料

> 务必在实验前认真阅读《实验说明 2019》《attacklab.pdf》《README-attacklab.txt》，之后再进行实验。磨刀不误砍柴工！

2.5 尝试攻击

- 仔细观察反汇编代码，解出每个攻击的代码
- 将内容写入文本文件（如 `attack_c1.txt`），每两位间加入空格
- 进行攻击。攻击前将文本文件通过 `hew2raw` 转为真正的十六进制文件，作为 `ctarget` 的输入。

```
cat attack_c1.txt | ./hew2raw | ./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 GDB 调试

- gdb 运行程序

```
gdb ./ctarget
> set args < input
> run
```

- 分析每一段汇编代码
- 设置断点，运行至断点
- 查看寄存器、内存等

2.7 分数与提交

- 查看得分：http://192.144.238.229:15513/scoreboard
- 实验报告
  - 实验方法
  - 实验结果（完成度、攻击代码）
  - 详细过程
- 祝大家实验愉快(´▽`)