# Attack Lab 实验说明2023

## 实验要求和内容

- 可执行文件 `ctarget` 和 `rtarget` 是本次实验的题目可执行文件，其中共包括5个phase：
  - `ctarget` 的3个phase为代码注入攻击。在 `ctarget` 中栈空间地址是固定的（每次启动时栈地址保持一致），并且栈空间中的数据是可执行的。
  - `rtarget` 的2个phase是ROP攻击。在 `rtarget` 中栈空间地址是随机的（每次启动都不一样），并且栈空间的数据是不可执行的。

  你需要做的是通过各种方法让程序非正常执行（调用特定函数），详情见官方说明文档。
- 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过程（但不鼓励篇幅过长）。

## 实验步骤

### 1. 登录服务器

服务器地址 `ics.ruc.rvalue.moe`，用 `ssh`：

```
ssh <u加学号>@ics.ruc.rvalue.moe
```

例如 `ssh u2023123456@ics.ruc.rvalue.moe`。

### 2. 下载文件

在服务器上用 `wget`：

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

选项 `-O` 后的参数 `"target.tar"` 可以替换为具体路径。

解压缩：

```
tar -xvf target.tar
```

你会得到一个名为 **targetN** 的目录，"N"是你的target的编号。

**注意：**

- 理论上你用浏览器访问 `ics.ruc.rvalue.moe:15513` 输入学号和邮箱也能下载target，但速度非常慢，几乎下载不了，因此建议直接在服务器上用 `wget` 下载。
- 即便你输入相同的学号和邮箱，每次下载的target**都是不同的**。因此**最好不要重复下载**。如果你下载了新的target，那么你在之前的target上做过的phase需要重做一遍，并且请在实验报告里注明target编号。

## 3. 反汇编

- 文件列表
  - `ctarget`：完成三个代码注入攻击的可执行文件。
  - `rtarget`：完成两个ROP攻击的可执行文件。
  - `cookie.txt`：用于验证身份，**不要更改**。
  - `farm.c`：rtarget的源文件之一，用于产生ROP攻击。
  - `hex2raw`：将用ascii 字符表示的十六进制数据转（转义）为攻击数据。它从标准输入读取以空格或换行分隔的十六进制表示的数据，将转义后的数据输出到标准输出。（例如字符串 `61 62 63` ，底层数据实际是 `0x36 0x31 0x20 0x36 0x32 0x20 0x36 0x33` ， 经过 `hex2raw` 输出真正的 `0x61 0x62 0x63` 共3个字节的数据）
- 反汇编
  - `objdump -d ./ctarget > ctarget.asm` ， `objdump -d ./rtarget > rtarget.asm`

## 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，里面几乎已经告诉你该怎么解这个实验，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 `ctarge.l1`），每两个十六进制位之间需要添加空格，可以换行和注释。
- 进行攻击。攻击时，你需要使用 hex2raw 将你的文本文件转换为原始字节流数据，作为 target 的输入

  ```
  cat ctarget.l1 | ./hex2raw | ./ctarget
  ```

  其它诸如怎么用gdb启动参见 **attacklab.pdf** 。
- 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、下载的 target.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：attacklab实验报告+学号.pdf
  - 你的 `target.tar`
  - 攻击串文件按题目顺序依次命名为： `ctarget.l1`， `ctarget.l2`， `ctarget.l3`， `rtarget.l2`， `rtarget.l3`。