中南大学

《SEED PROJECT》
实验报告

学生姓名 王雅琪

指导教师 王伟平

学　　院 信息科学与工程学院

专业班级 信息安全 1402

学　　号 0906140226

完成时间 2016.12

实验一 Heartbleed Attack Lab

一、实验目的

通过实验了解心脏滴血攻击的原理和过程，加深对 SSL 协议的理解，增强动手实践能力。

二、实验内容

在 SEED Project 网站的指导下，通过查询资料，独立完成心脏滴血攻击实验。

三、实验原理

1、心脏滴血攻击：OpenSSL 软件存在“心脏出血”漏洞，攻击者能够从服务器内存中读取最多 64KB 的数据，心脏滴血攻击原理：客户端向服务器发送的询问包中有一个域存放了该包的字节数，但是这个域的值可由客户端进行设置，服务器收到询问包后，将内容放入内存，发送应答包，直接将询问包中的字节大小作为应答包的大小，并没有对该大小进行验证。服务器按照该字节大小从内存中提取内容，若客户端声称的包长度大于实际长度，则服务器中的其他信息会被随机的发送给客户端，造成信息泄露。

2、 OpenSSL:OpenSSL 是一个安全套接字层密码库，囊括主要的密码算法、常用的密钥和证书封装管理功能 SSL 协议，SSL 是 Secure Sockets Layer（安全套接字）的缩写，可以在 Internet 上提供秘密性传输。

3.Heartbleed bug (CVE-2014-0160)是旧版本的 Openssl 库中一个的一个漏洞。利用这个漏洞，攻击者可以从服务器里窃取一部分随机数据。这个漏洞主要是源于 Openssl 设计的协议继承了 Heartbeat 协议，使用 SSL/TLS 来保持连接的实时性、保活性。

原理示意图如下：

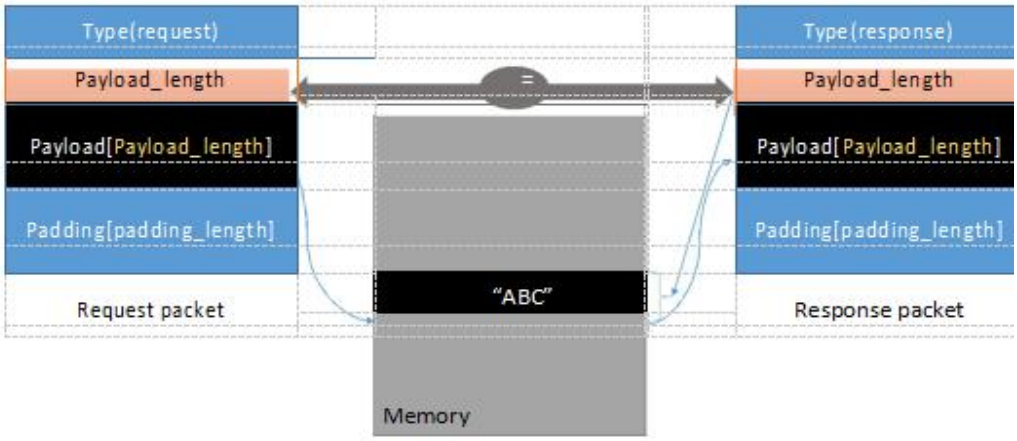


Figure 2: The Benign Heartbeat Communication

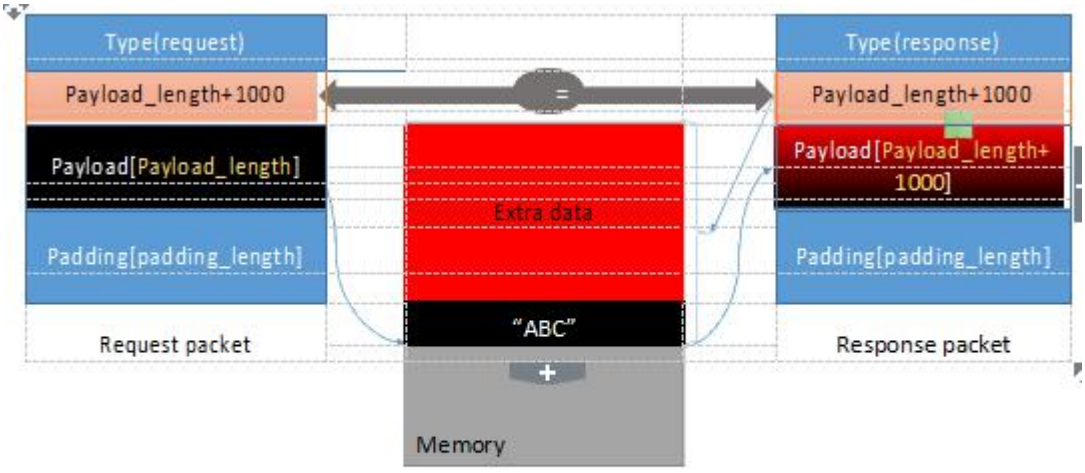


Figure 3: The Heartbleed Attack Communication

四、实验过程

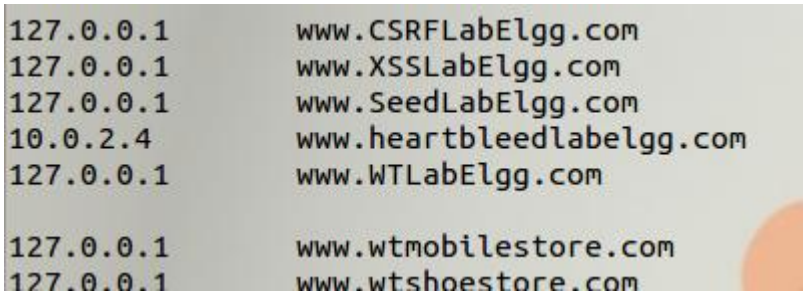
1、搭建实验环境

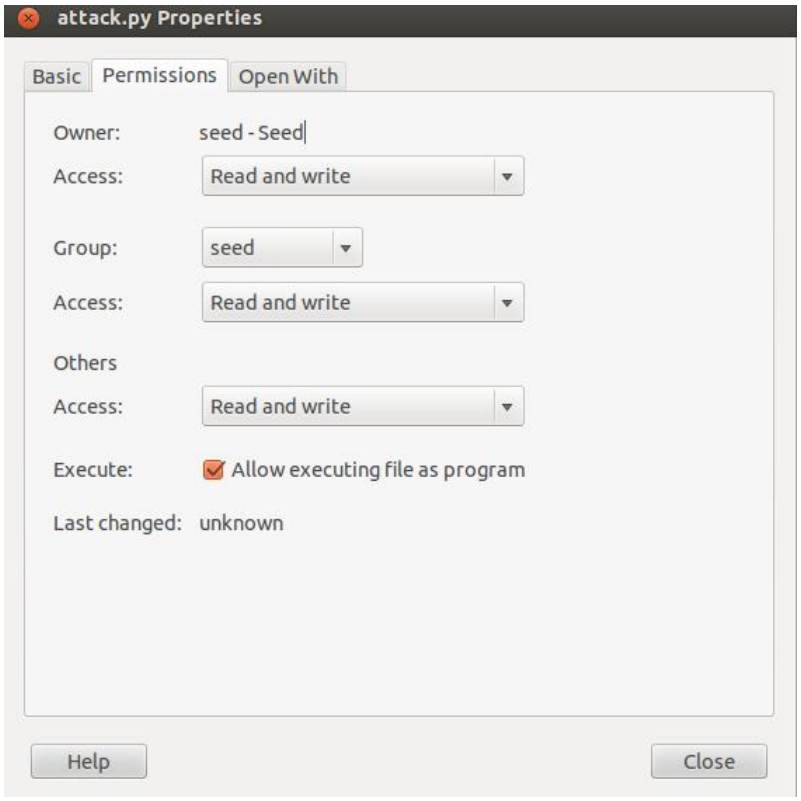
按照 description 安装虚拟机及 Ubuntu，新建一个虚拟机，取名为 attacker，以 attacker 为模板克隆出 victim，如图所示

2、了解心脏协议

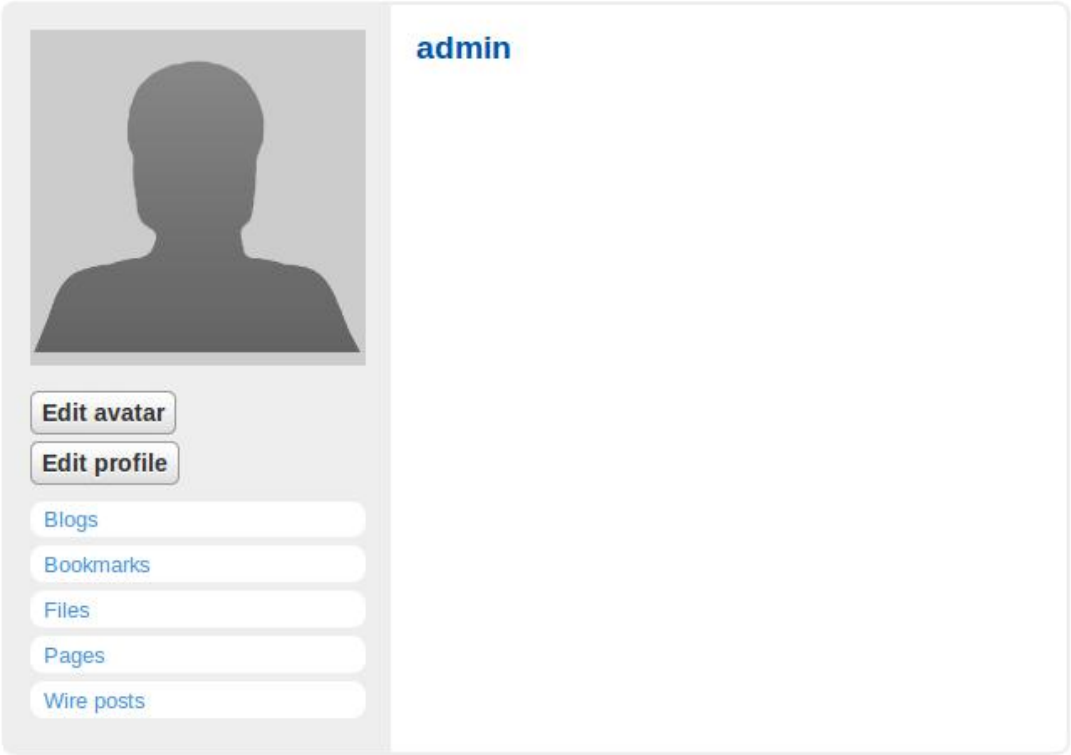
心脏协议有两种信息类型，一种是请求包，一种是应答包。用户向服务器发送一个请求包以验证和服务器的连接是否还存在，服务器收到询问包后，服务器将询问包的内容放入内存，若连接还存在，服务器向客户端发送一个和请求包同样大小的应答包，内容从内存中提取。

3、修改权限和 IP



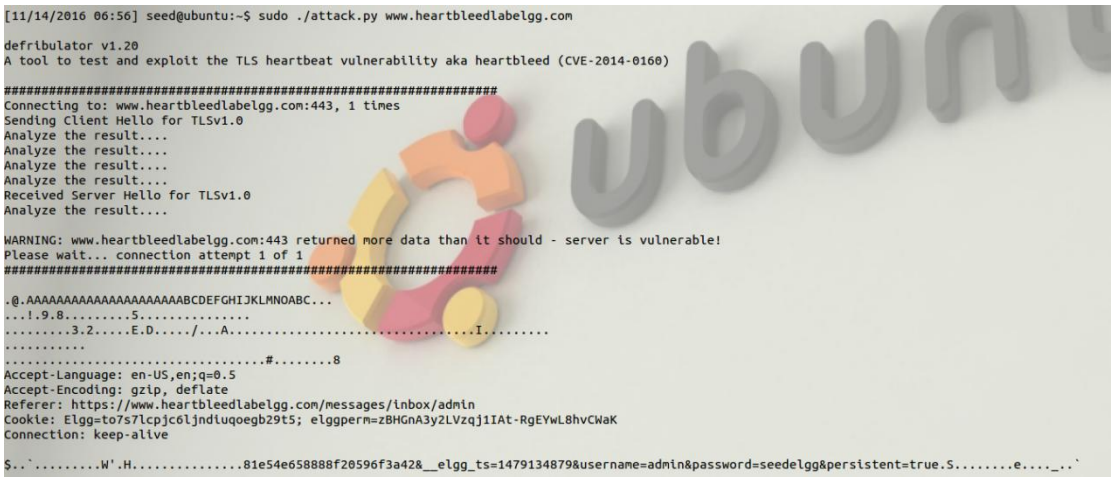


4、以管理员身份登录，并向好友 Boby 发送消息



5、发动攻击

（1）获取到登录名和密码

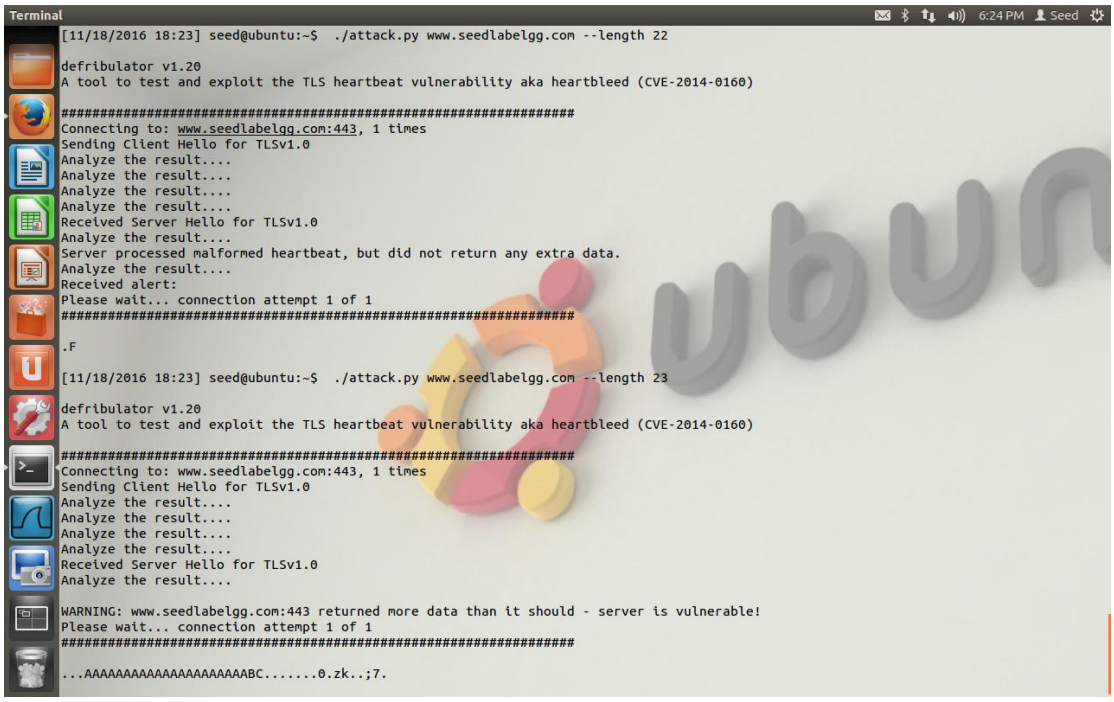


（2）获取到想 Boby 发送的信息

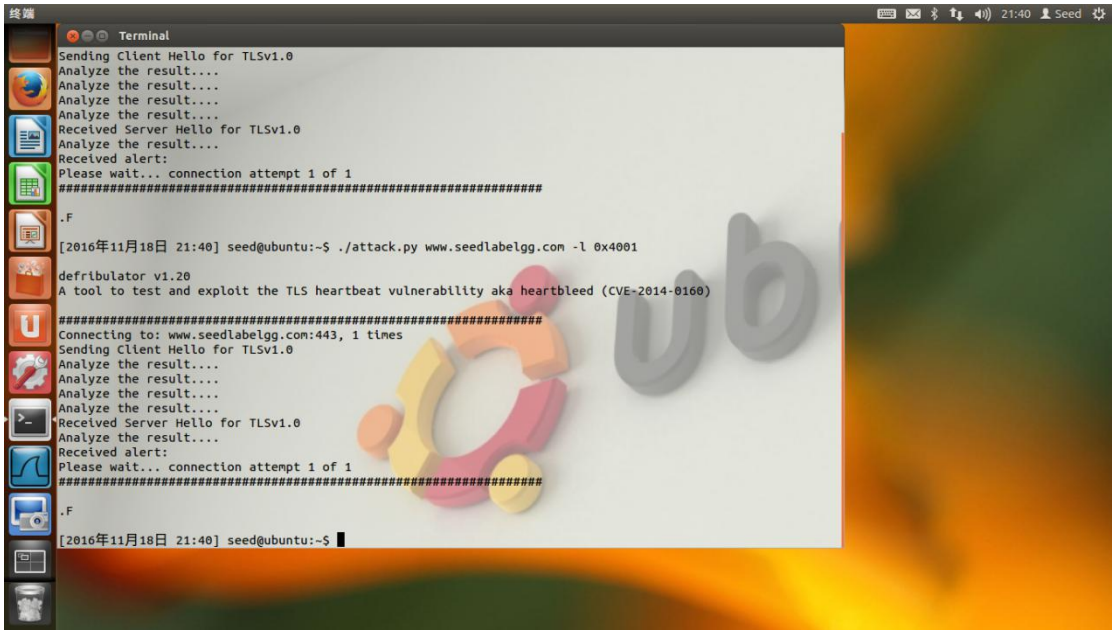
6、修改 length 值，再次攻击

Length 值为 660 时，可完整的获取信息：thank you for your help

7.寻找一个边界值，使得查询接收响应包而不附加任何额外的数据。
（通过实验找到的边界值为 23）

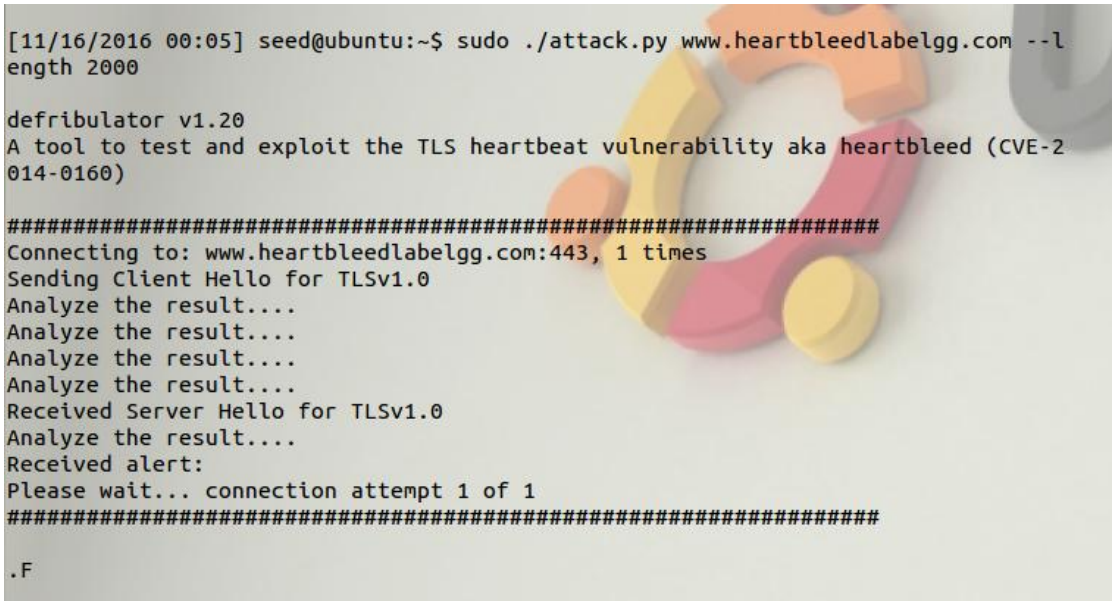


寻找边界值



寻找边界值

8、更新 OpenSSL 后，漏洞被修复，再次攻击时发现漏洞不存在



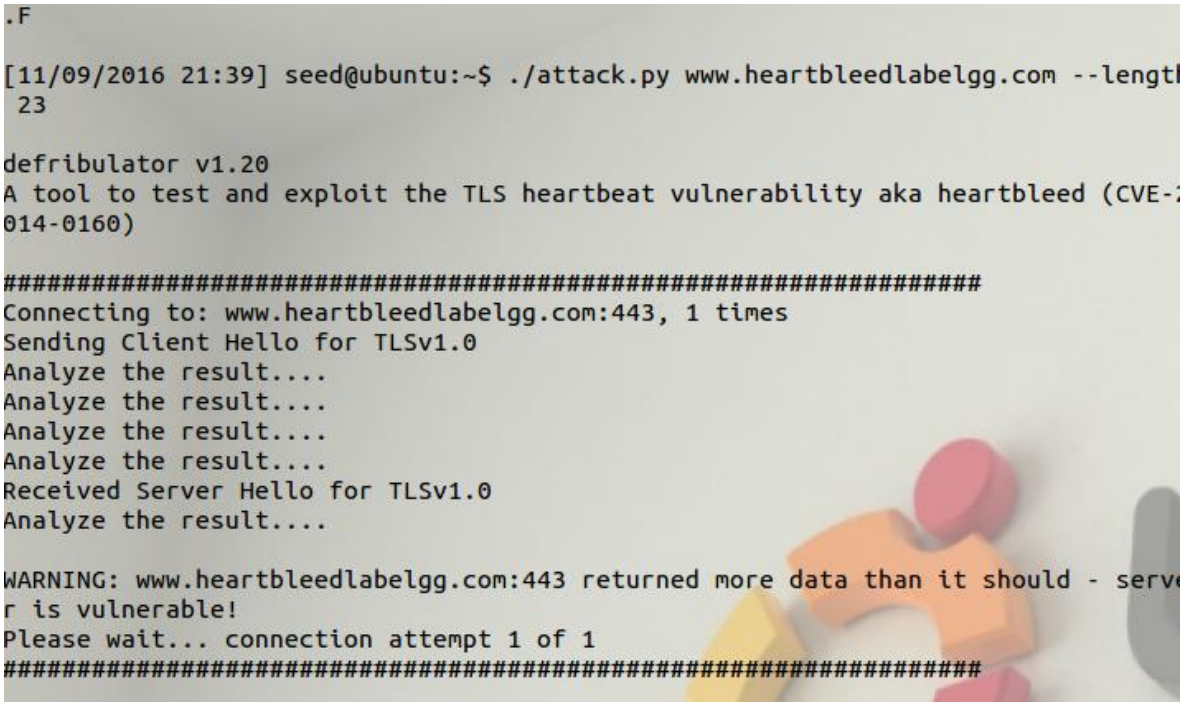
五、实验结果以及讨论

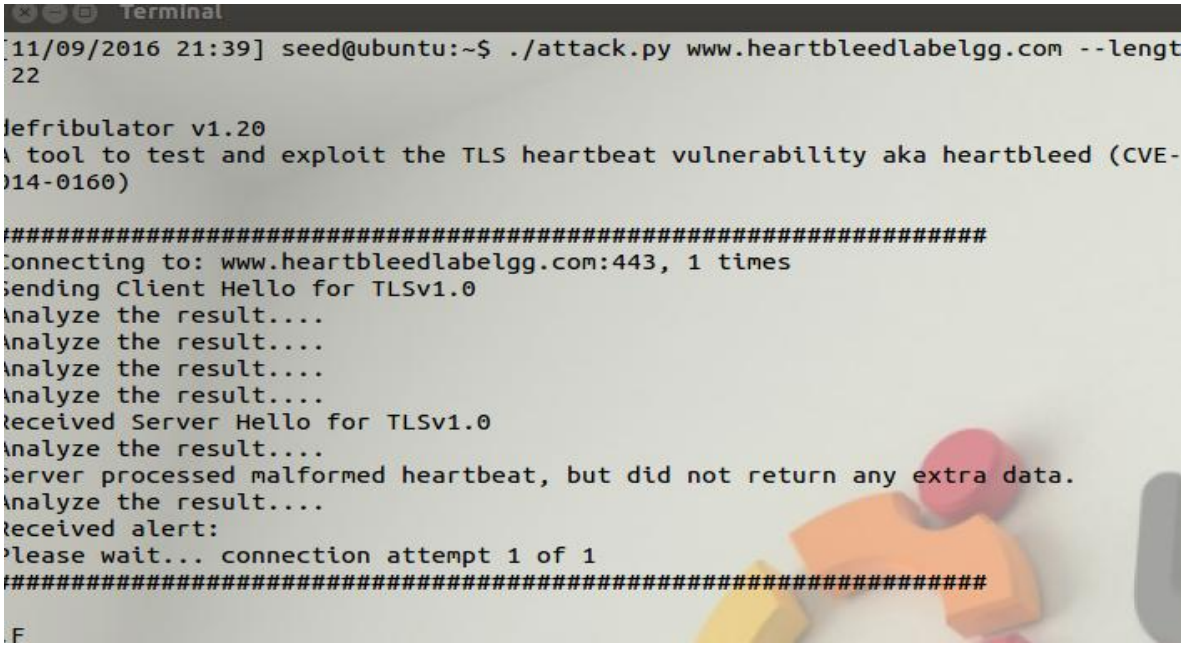
按照实验指导完成 Task1 之后，下载脚本到计算机并运行之后，就可以观察到

```
_elgg_token=a92c2d107179d03162ad69a3eeb306da&__elgg_ts=1478702623&username=admin&password=seedelgg.:......0......c..>
```

成功捕获到了用户名以及密码。

在 task2 中，设置长度为 22 和 23 时返回消息分别如下所示：





对于问题 2.1，由观察的结构可以得知，边界值为 23
对于问题 2.2.，当缩短指定的长度时，返回的数据包长度也会相应的缩短。
在 Task3，更新更新到最新版本的 OpenSSL 库时，指定数据包的长度就会不起作用了，补丁已经打好了。