中南大學
CENTRAL SOUTH UNIVERSITY

网络安全

实验报告

学生姓名　　霍曼妍

学　　号　　0906140210

专业班级　　信息安全 1402

指导教师　　王伟平

学　　院　　信息科学与工程学院

完成时间　　2016 年 12 月

实验一　　HeartBleed Atrack

一、实验目的

首先需要了解心跳协议的工作过程，并且通过实验了解心脏滴血攻击的原理和过程，加深对 OPENSSL 协议的理解，增强动手实践能力。

二、实验内容

了解心跳协议的工作过程，在 SEED Project 网站的指导下，通过查询资料，并且利用网站上的资源，独立完成心脏滴血攻击实验。

三、实验原理

1.心跳协议：心跳协议（即 keepalive 协议）包含两种类型的信息，心跳请求包和心跳回应包。

2.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。

3.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及 SSL 协议，SSL 是 Secure Sockets Layer（安全套接层协议）的缩写，可以在 Internet 上提供秘密性传输。

四、实验环境

Oracle VM VirtualBox

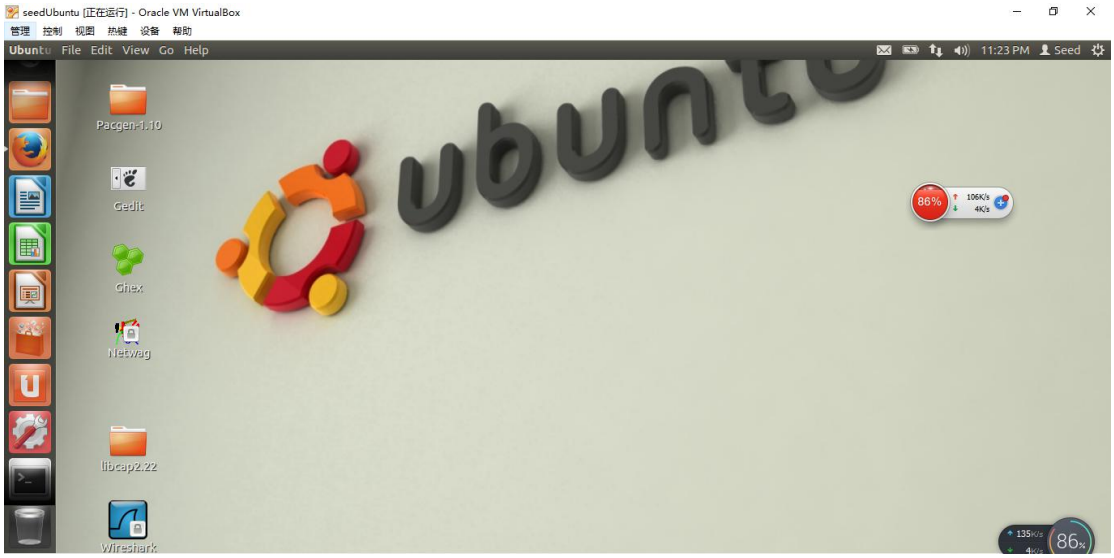
Ubuntu12.04

五、实验过程

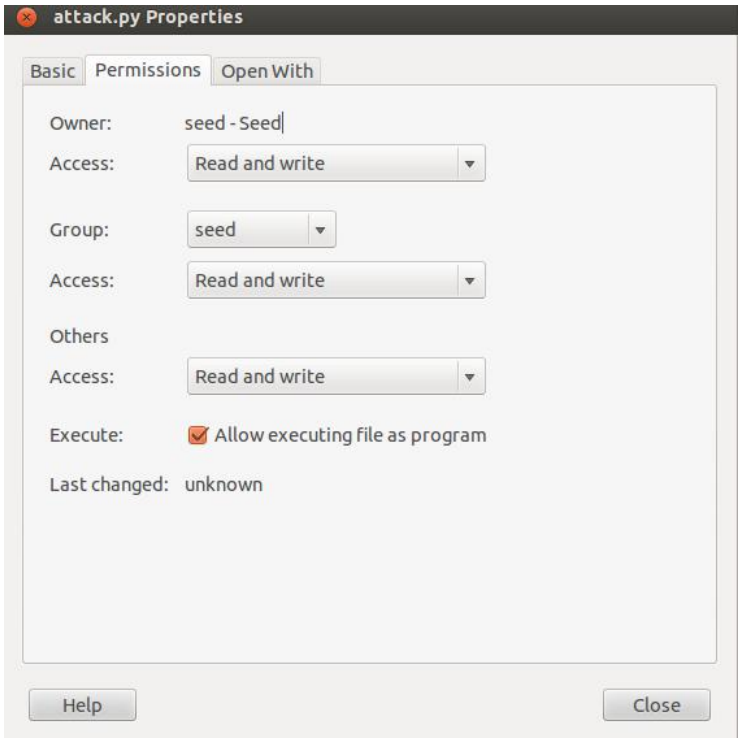
1、搭建实验环境

按照 description 安装虚拟机及 Ubuntu，新建一个虚拟机，取名为 seedUbuntu，如图所示：

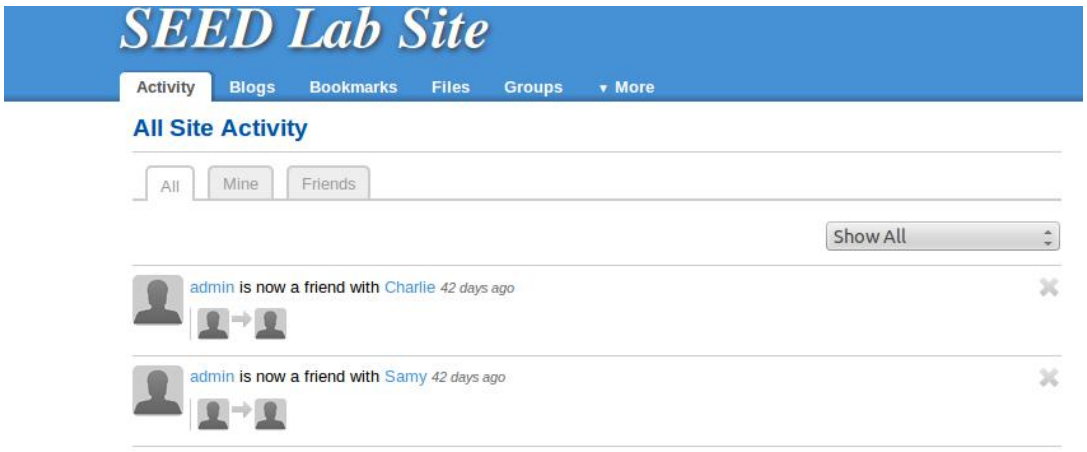
运行 seedUbuntu 后，如图所示：



2. 在实验室下载了 attack.py 后改变属性，使其可以运行：

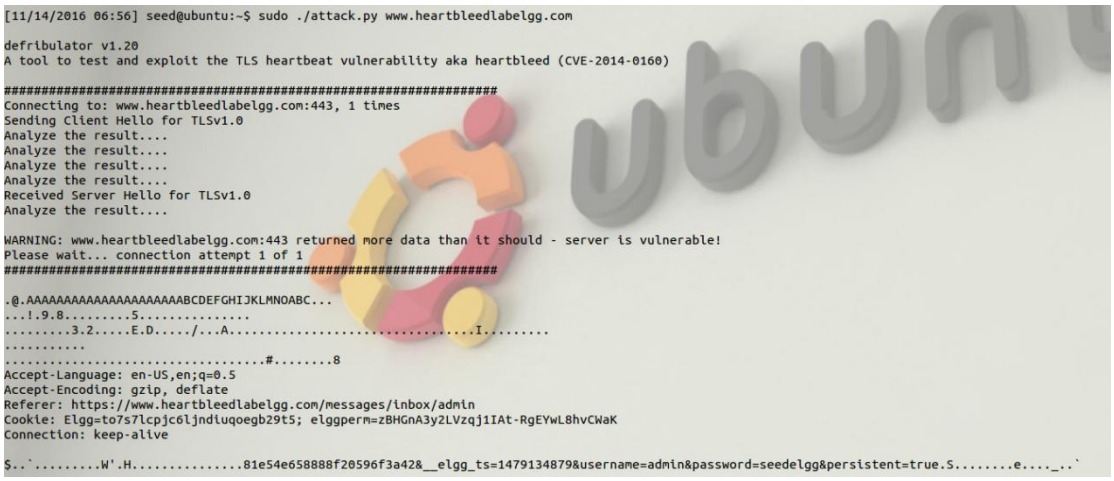


3. 在浏览器登录实验室专用页面后，添加用户以及与其他用户通信，确保添加内容进网页服务器中：



4. 发动攻击

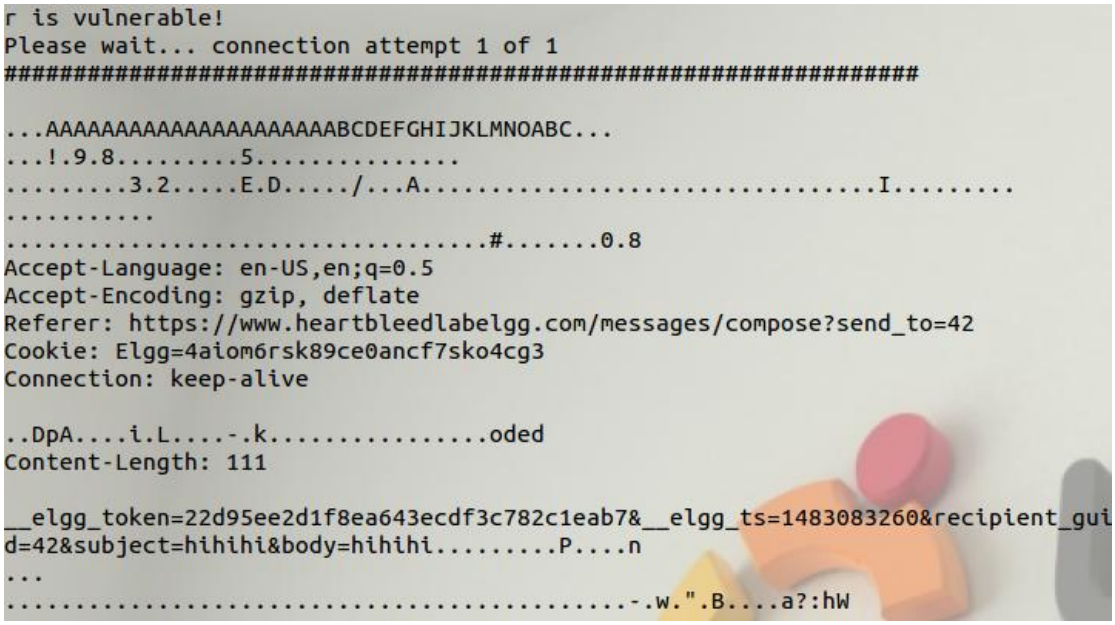
（1）获取到登录名和密码



（2）获取到向 samy 发送的信息

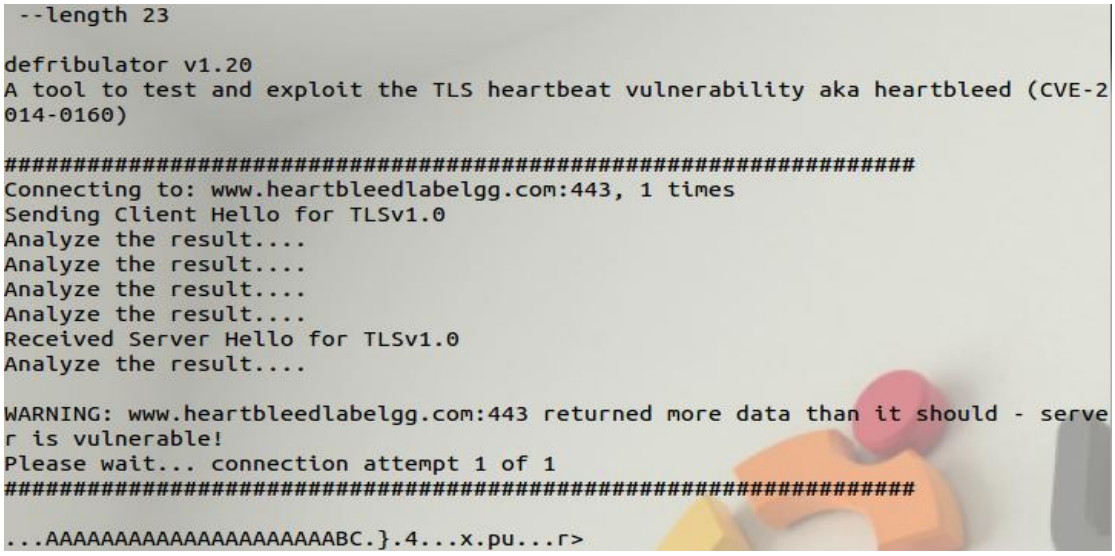
5. 修改 length 值，再次攻击

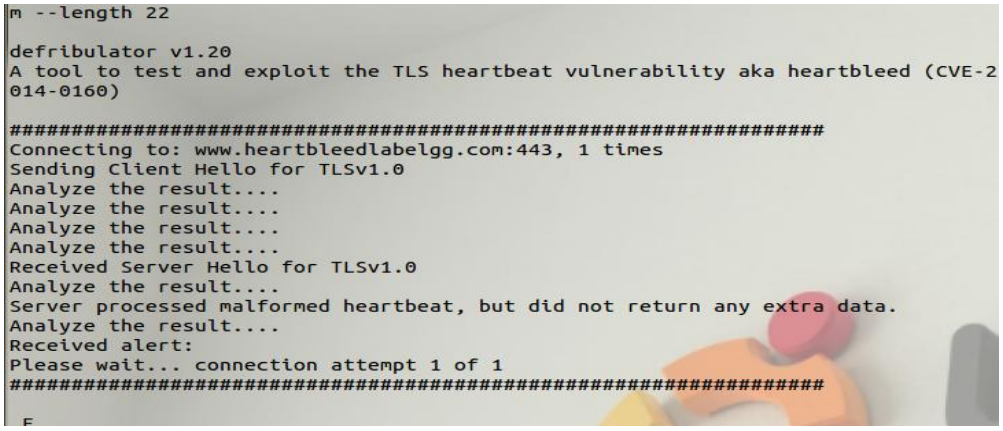
Length 值为 660 时，可完整的获取信息：hihihi



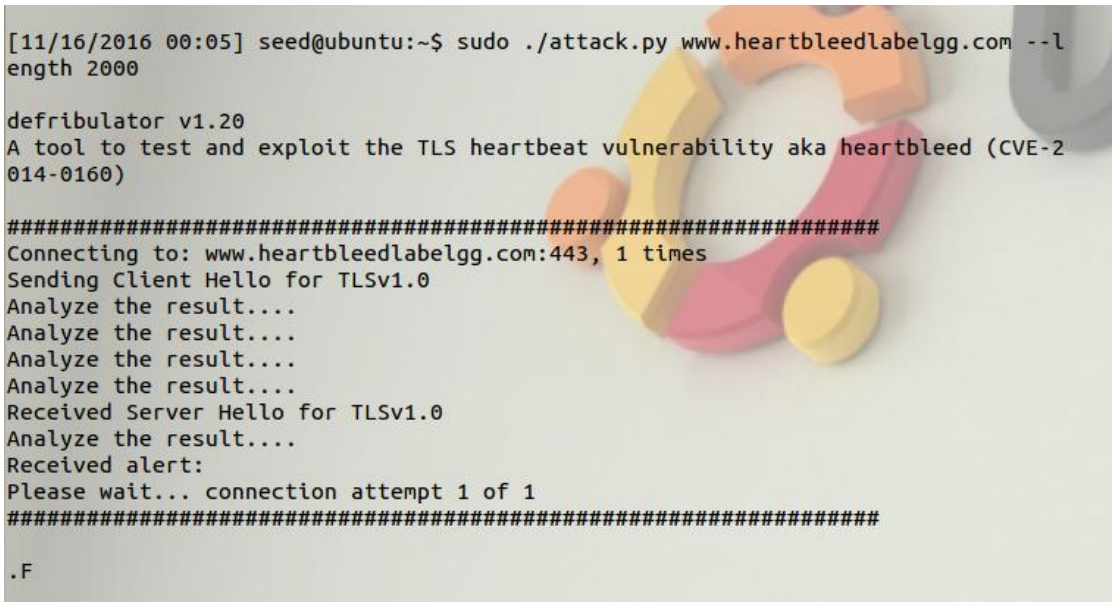
修改 length 为 500，很难获取有用的信息

6. 依次减小 length 长度，找到临界值，不能在获取任何有价值的信息，但是漏洞依然存在，临界值为 22



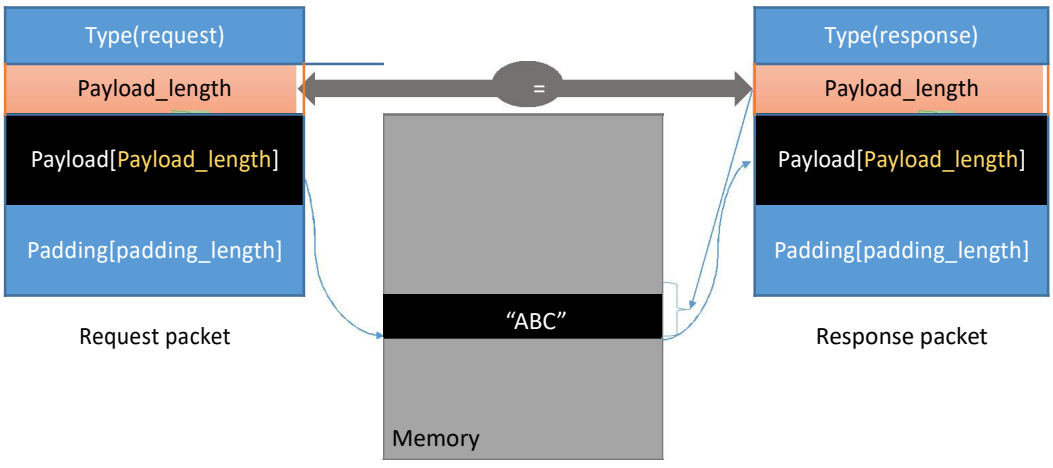


6、更新 OpenSSL 后，漏洞被修复，再次攻击时发现漏洞不存在

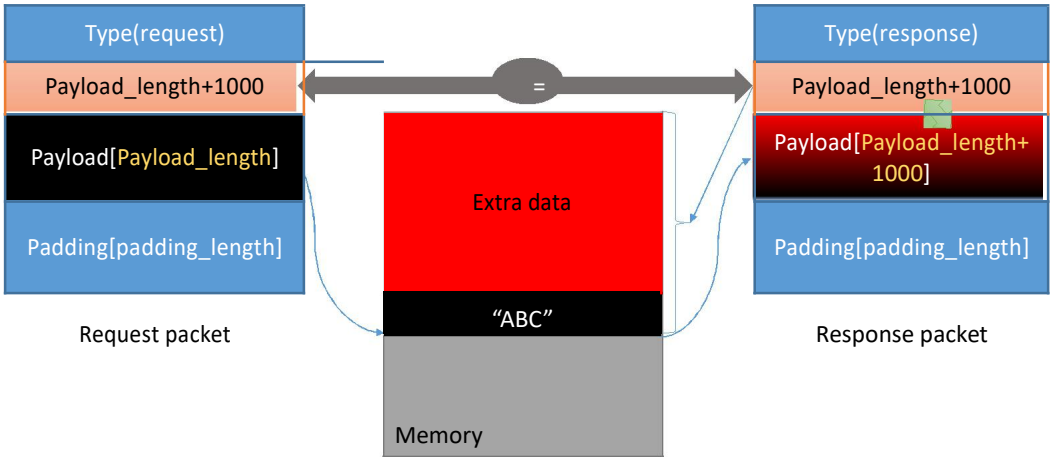


六. 攻击原理分析

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。具体如下图：



正常交流时的对话状态



使用心脏滴血攻击时的交流过程

七. 实验总结

通过此次试验，我对 SSL 协议中存在的一些缺陷有了更深的了解，同时对如何一个建立安全的通信通道有了自己的一番理解，对心脏滴血的攻击过程了解的更深刻，由于以前从未接触过 Ubuntu，但是通过查询资料，各种问题都得以解决，从而最终可以成功的完成实验。