中南大學
CENTRAL SOUTH UNIVERSITY

网络安全

实验报告

学生姓名 马田瑶

学　　号 0906140124

专业班级 信息安全 **1401**

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

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。

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

VirtualBox Ubuntu

五、实验过程

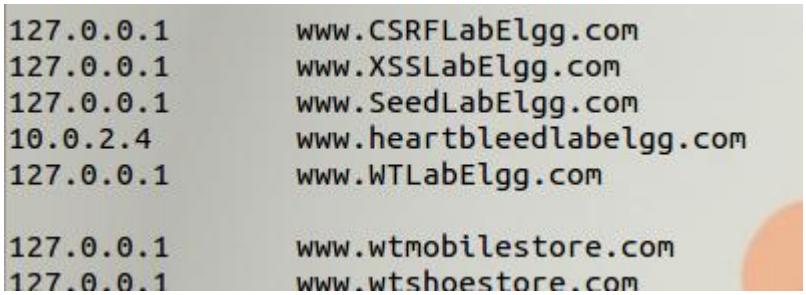
1、搭建实验环境

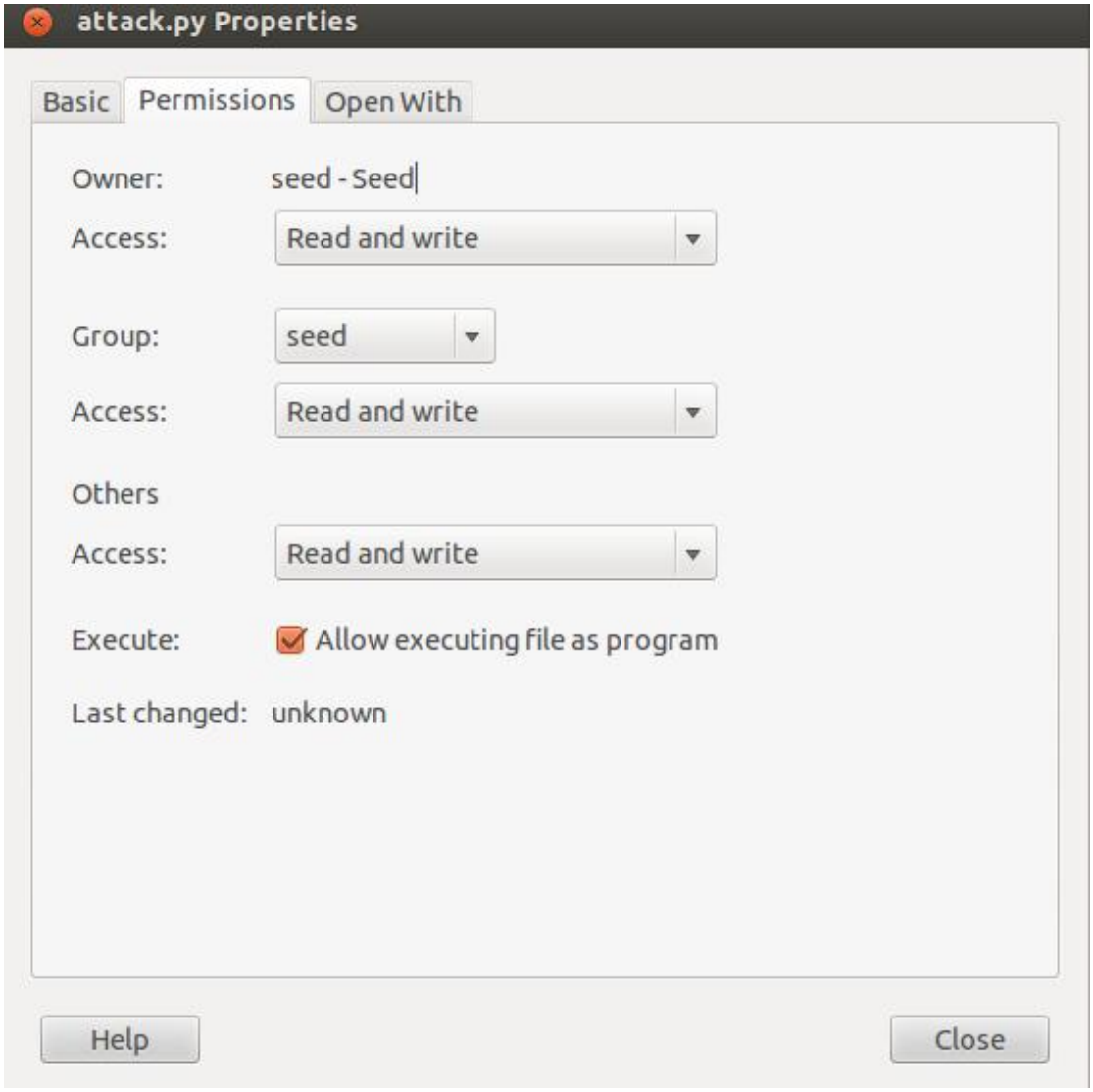
按照 description 安装虚拟机及 Ubuntu，新建一个虚拟机，取名为 attacker，以 attacker 为模板克隆出 victim，如图所示

2、了解心脏协议

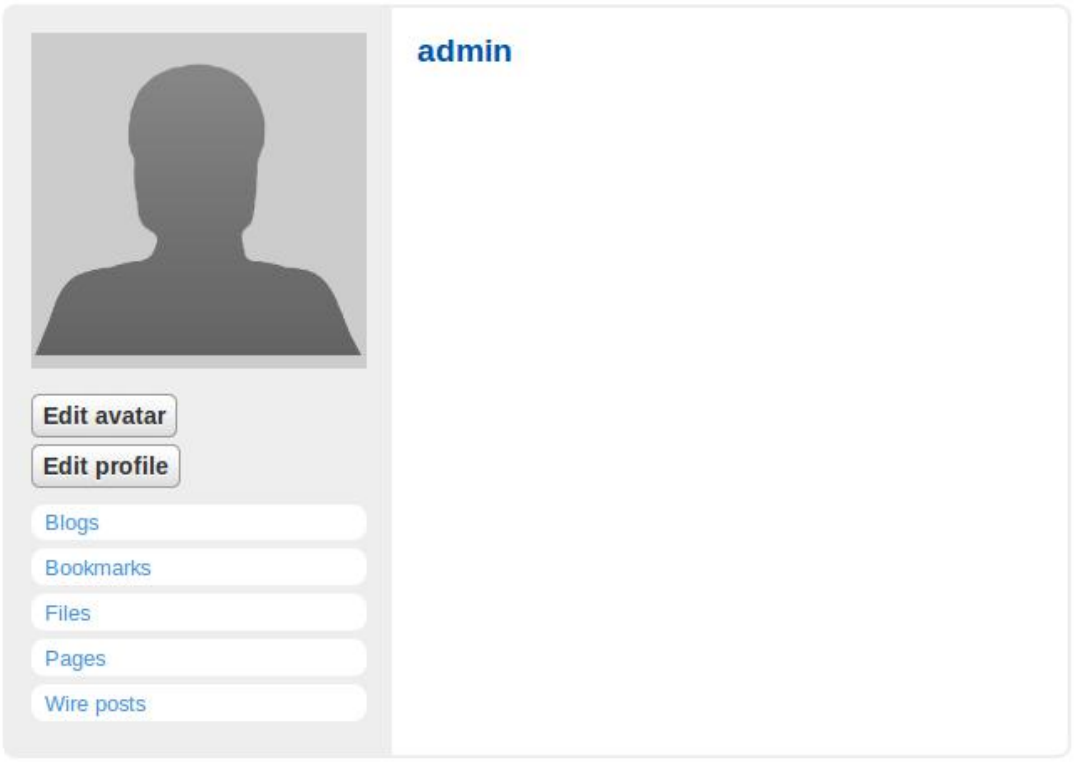
心脏协议有两种信息类型，一种是请求包，一种是应答包。用户向服务器发送一个请求包以验证和服务器的连接是否还存在，服务器收到询问包后，服务器将询问包的内容放入内存，若连接还存在，服务器向客户端发送一个和请求包同样大小的应答包，内容从内存中提取。

3、修改权限和 IP



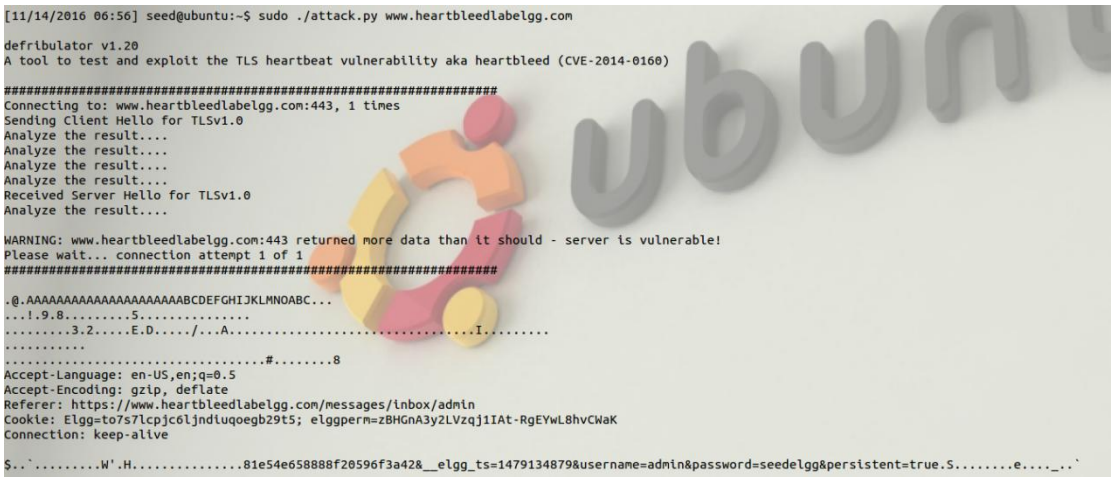


4、以管理员身份登录，并向好友 Boby 发送消息



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

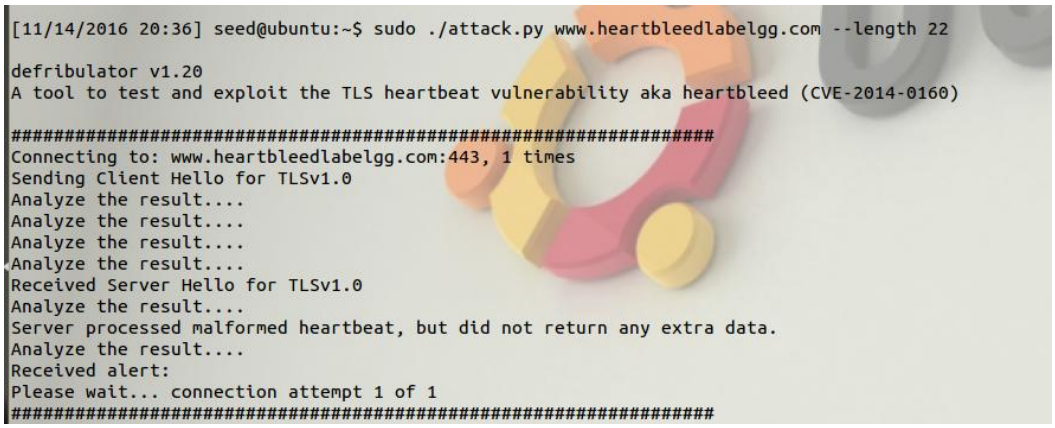
6、修改 length 值，再次攻击

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

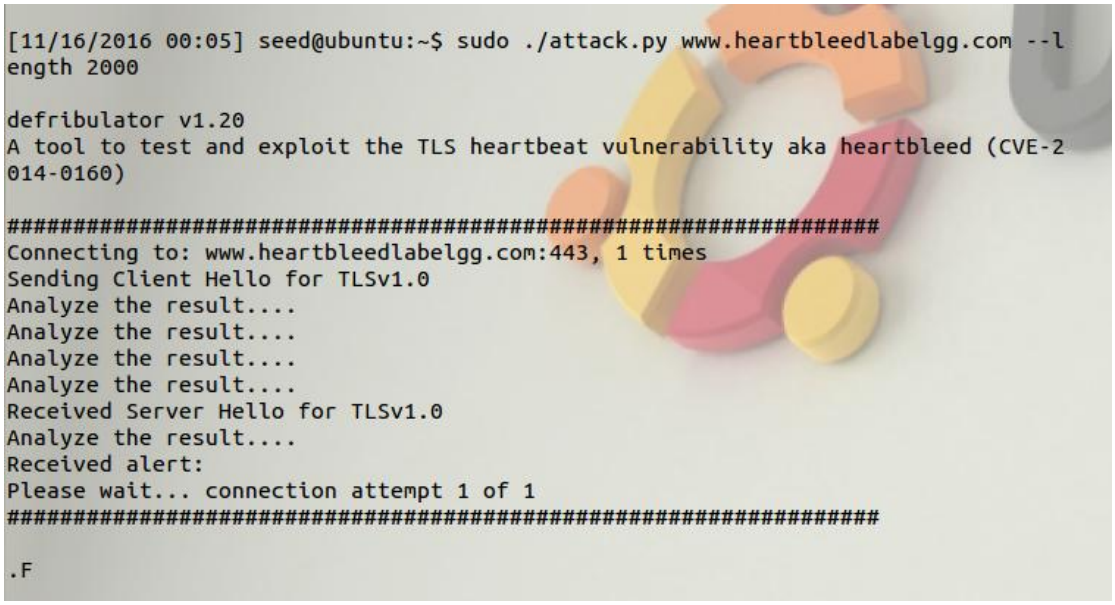
修改 length 值为 640 时，同一条消息不能再获取完整的信息

修改 length 为 600，很难获取有用的信息

7、逐次减小 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



8、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

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。

七、改进办法

在服务器端对客户端发送的询问包进行长度的验证。

六．实验总结

通过此次试验，我对 SSL 协议建立安全的通信通道有了更深的理解，对心脏滴血的攻击过程了解的更深刻，虽然以前没有使用过 Ubuntu，但是通过查询资料，各种得体都得以解决，最终可以成功的完成实验。