中南大學
CENTRAL SOUTH UNIVERSITY

网络安全网上学习实验报告

题　　目：	网络安全网上学习实验报告
学生姓名：	唐　轩
学　　号：	0906140202
指导教师：	王伟平
学　　院：	信息院
专业班级：	信安 1402

实验一　Heartbleed 实验

一、实验背景

心脏出血漏洞（英语：Heartbleed bug），也简称为心血漏洞，是一个出现在加密程序库 OpenSSL 的程序错误，首次于 2014 年 4 月披露。该程序库广泛用于实现互联网的传输层安全（TLS）协议。只要使用的是存在缺陷的 OpenSSL 实例，无论是服务器还是客户端，都可能因此而受到攻击。此问题的原因是在实现 TLS 的心跳扩展时没有对输入进行适当验证（缺少边界检查），因此漏洞的名称来源于“心跳”（heartbeat）。该程序错误属于缓冲区过读，即可以读取的数据比应该允许读取的还多。

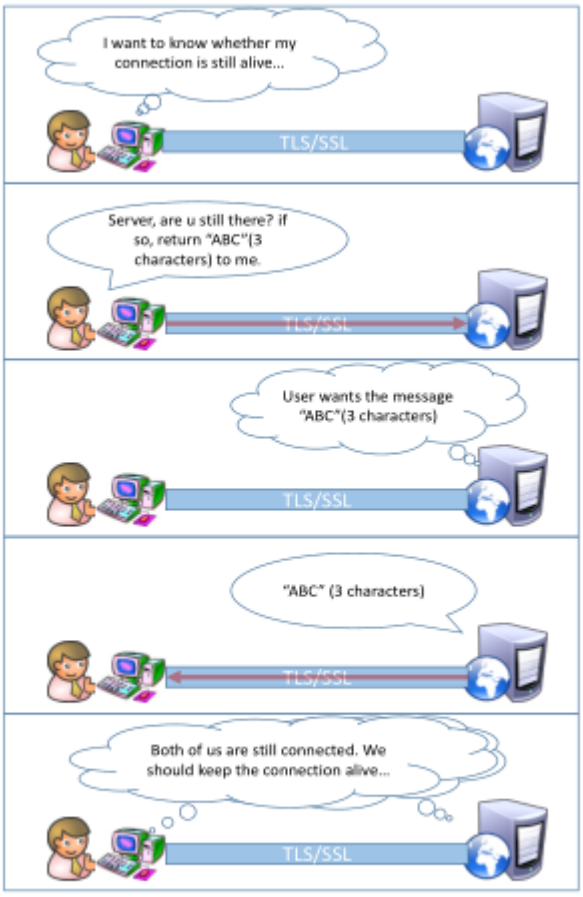


Figure 1: Overview of the Heartbeat Protocol

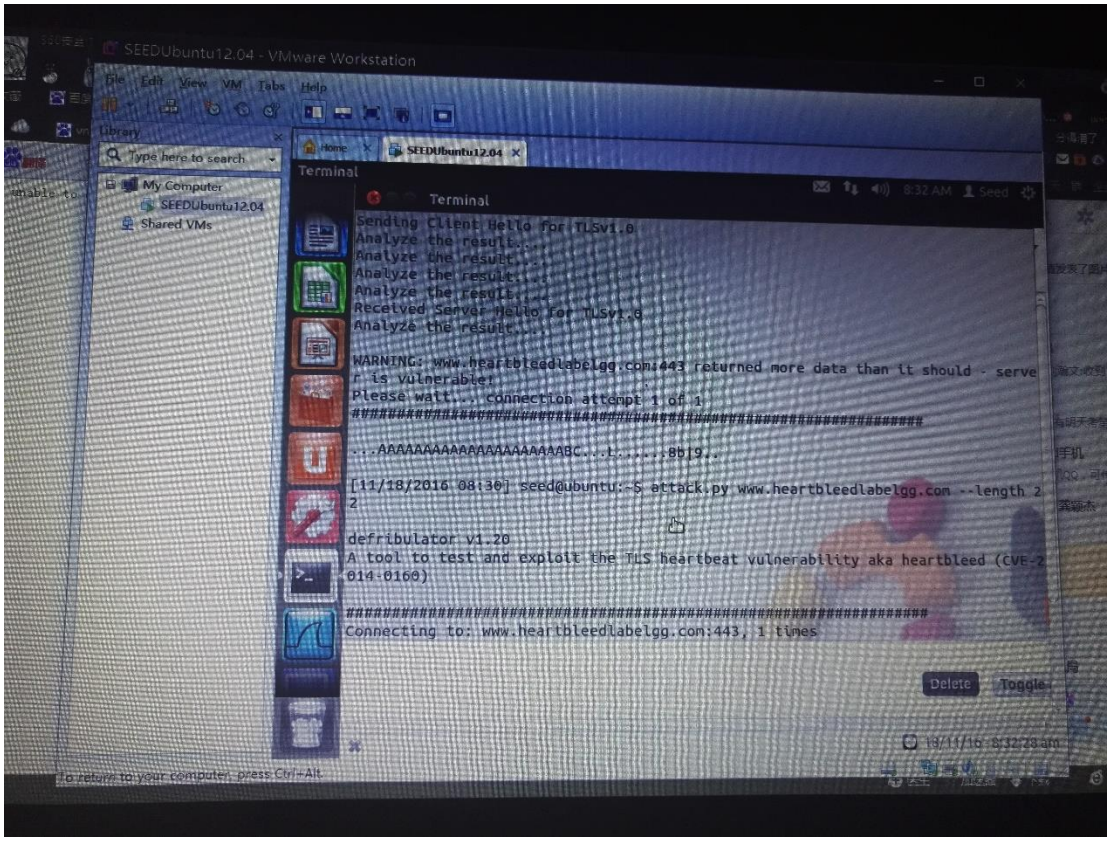
二、实验环境及过程

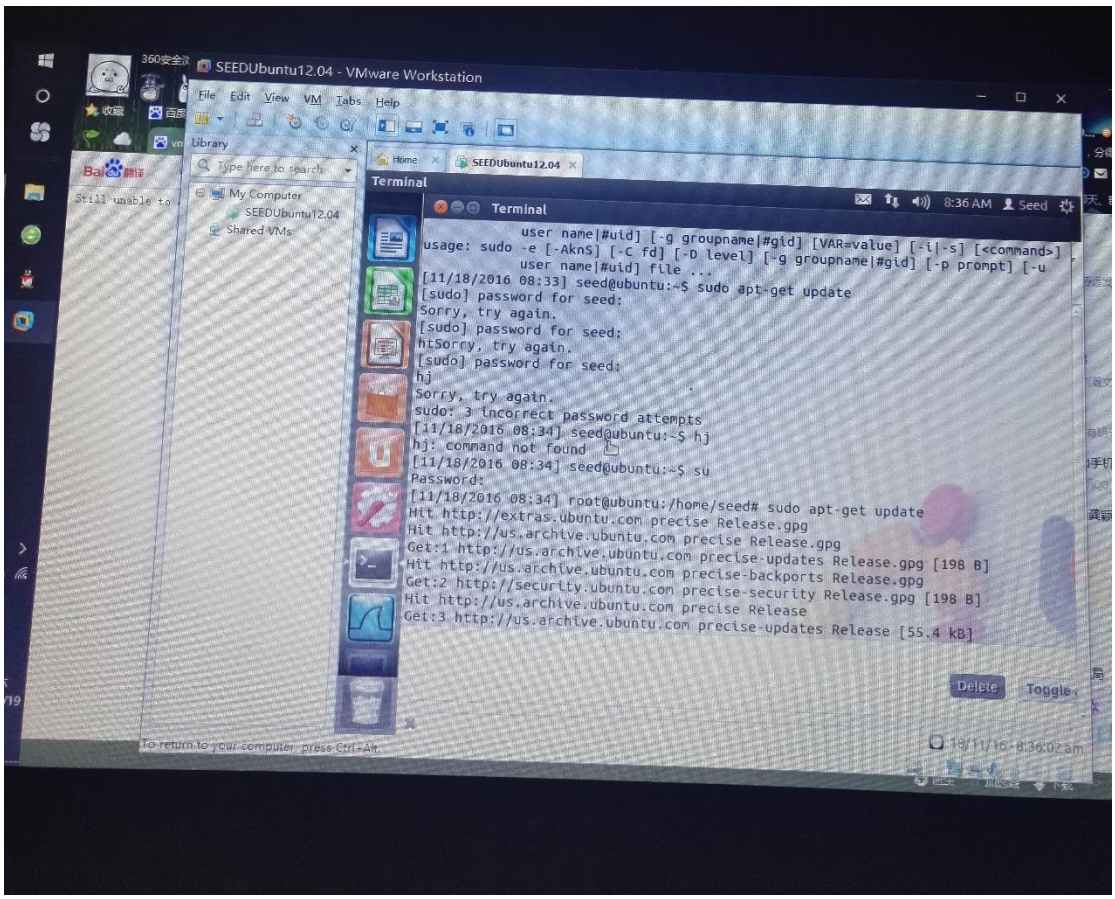
实验环境为在 VM 虚拟机中运行的 SEEDUbuntu12.04 系统（系统已经由实验室配置好环境）。

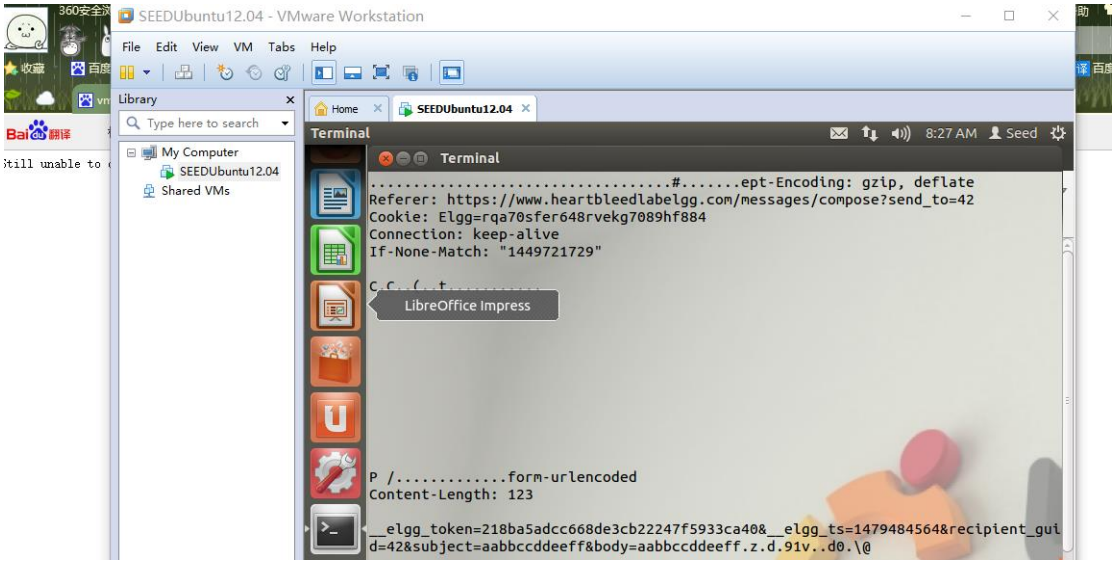
实验过程参考该实验下提供的 PDF 的实验指导书完成。

三、实验过程

1.按要求在网站发送邮件，再通过该漏洞对邮件内容进行捕获，获取详细信息。







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。

四、实验总结

通过此次实验，了解 Heartbleed 攻击的危害，方式及解决方法，使自己对网络安全有一方面的认识和了解，同时学会使用 SEEDLABS 网站进行网络安全的网上学习，提高自主学习的能力。