实验一　Heartbleed 实验

一．实验目的

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。

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。

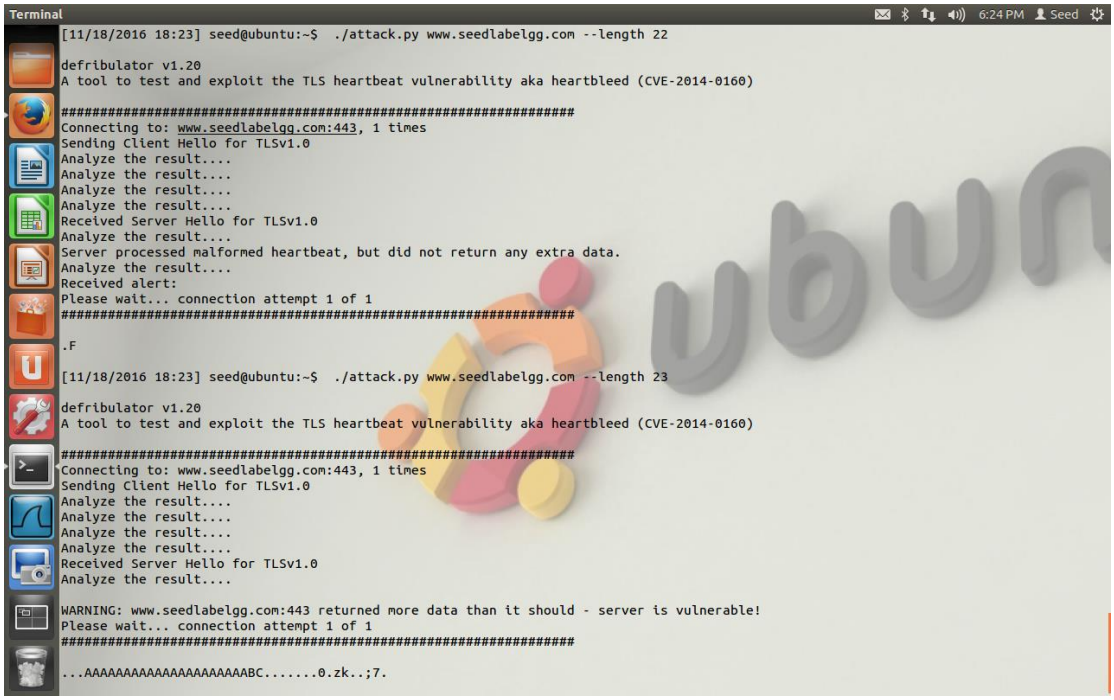
详细过程略

三．实验结果

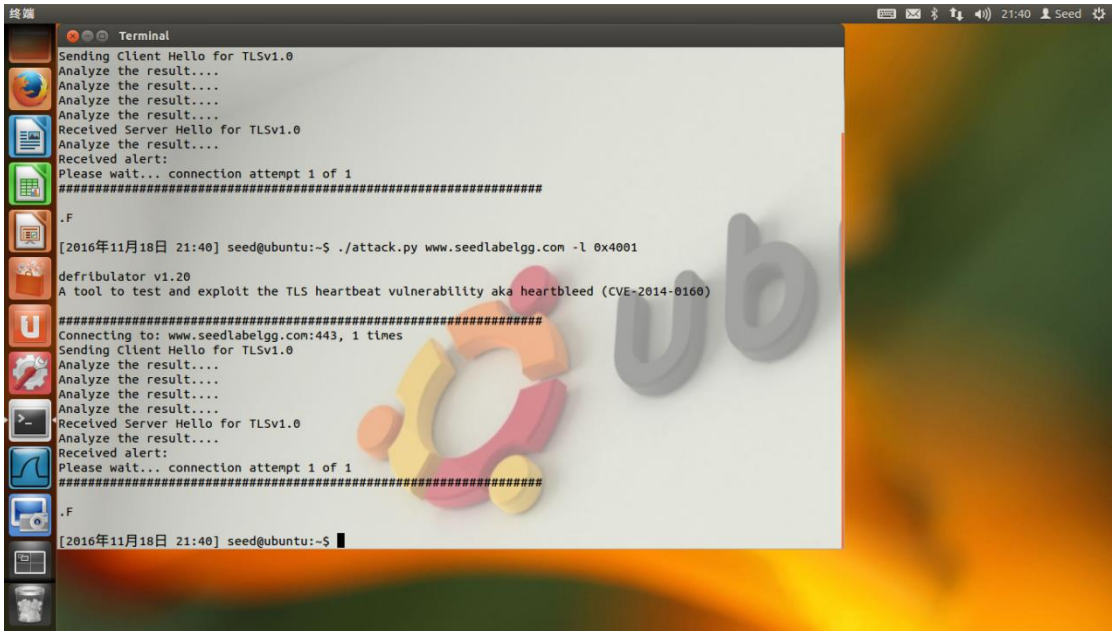
1.按要求在网站发送邮件，再通过该漏洞对邮件内容进行捕获，获取详细信息。（发送的邮件正文为 “HELLO WORLD”）

邮件截取内容

2. 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


终端
21:40
Seed
Terminal
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....
Received alert:
Please wait... connection attempt 1 of 1
.F
[2016年11月18日 21:40] seed@ubuntu:~$ ./attack.py www.seedlabelgg.com -l 0x4001
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
Connecting to: www.seedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....
Received alert:
Please wait... connection attempt 1 of 1
.F
[2016年11月18日 21:40] seed@ubuntu:~$

寻找边界值