网络安全网上实验

实验报告

学生姓名 何安东

学　　号 0906140208

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 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

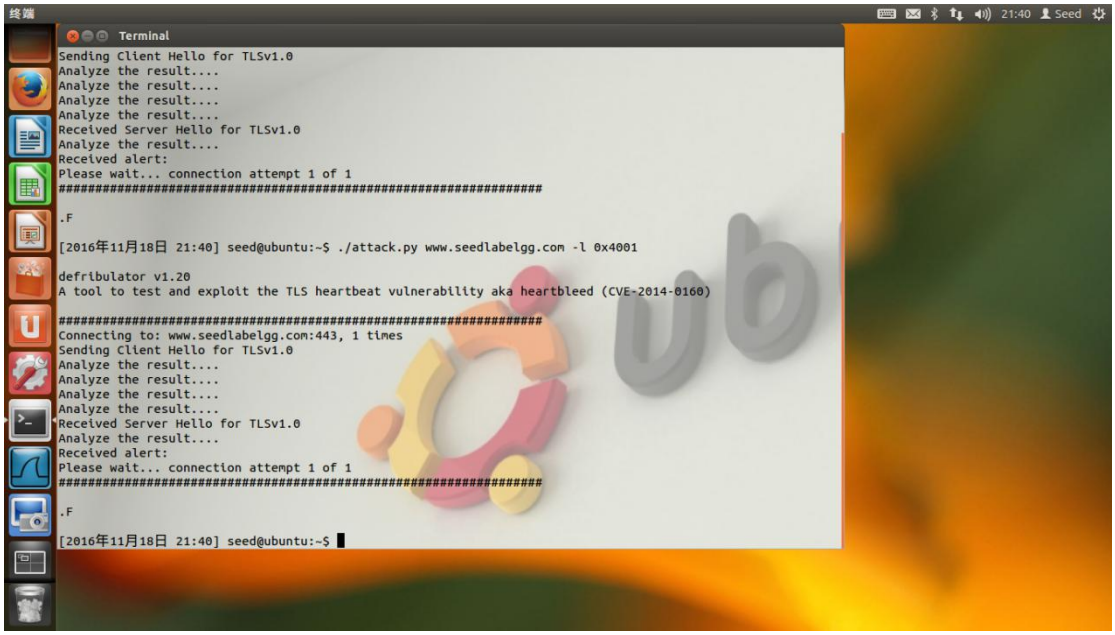
三．实验结果

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

实验一　Crypto_Hash 实验

一. 实验目的

通过此次实验，了解 Crypto_Hash 哈希加密的方法，使自己对哈希函数散列值和消息认证码有一定的认识和了解,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

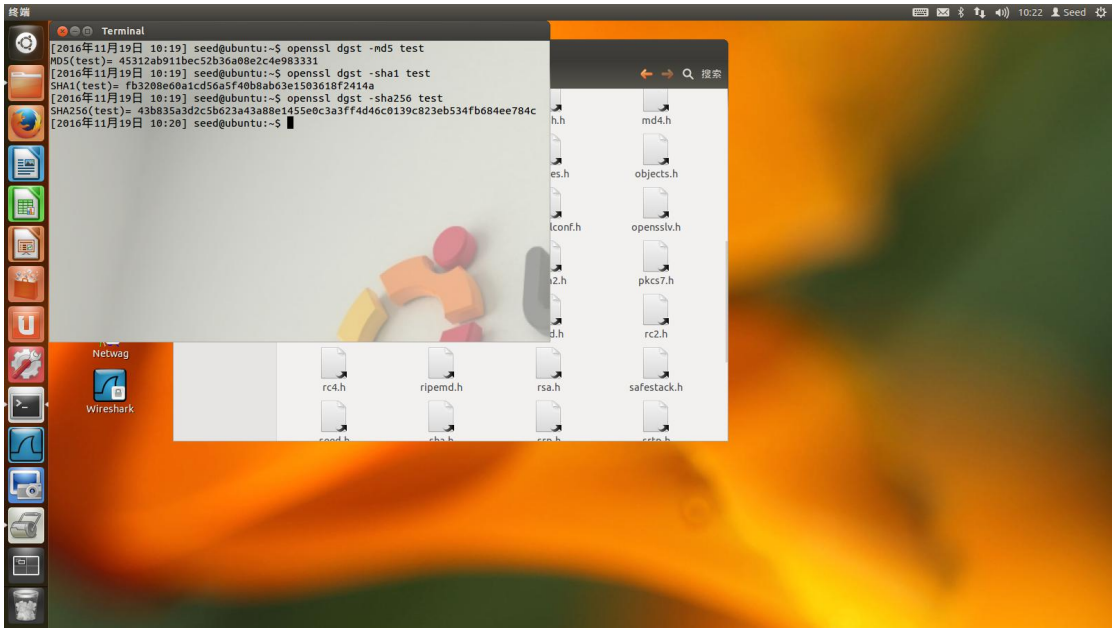
实验环境为在 VM 虚拟机中运行的 SEEDUbuntu12.04 系统（系统已经由实验室配置好环境）。

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

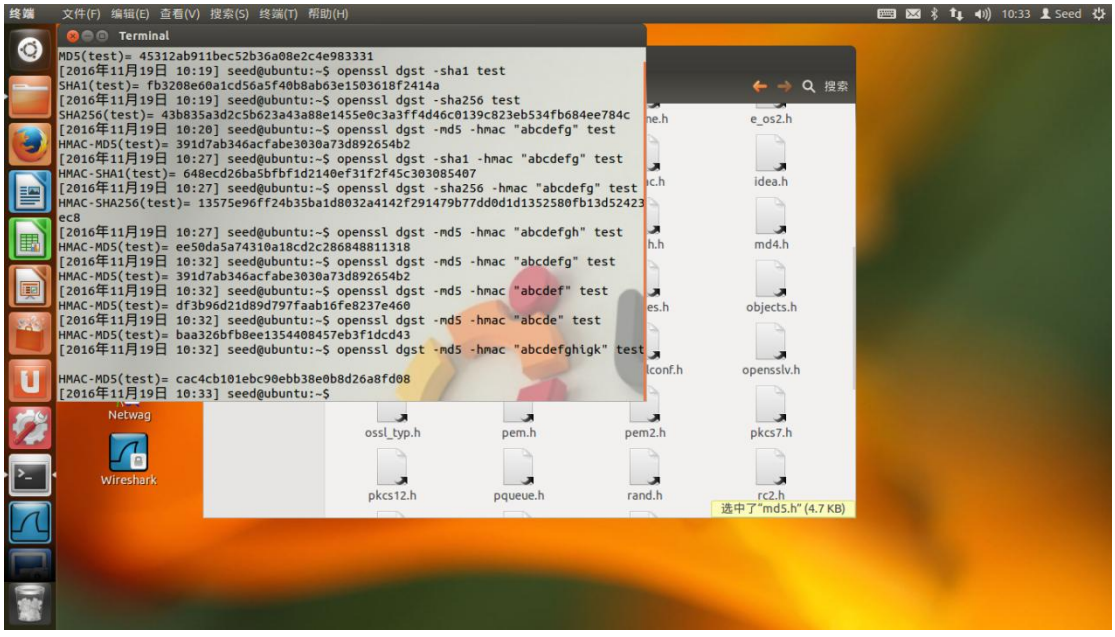
三. 实验结果

1.对指定的文件进行加密，获取信息摘要和认证码。至少使用三种不同的加密算法（如-md5, -sha1, -sha256 等）



加密同一文件得到不同 MAC

2. 对同一文件利用同一种算法进行关键字长度不同的 HMAC 散列函数进行加密，获取信息摘要和认证码



不同长度的加密得到不同 MAC

实验总结

通过此次实验，我对 Heartbleed 漏洞有了一定的认识，了解了利用该漏洞的攻击手段及修复方式，进行了简单的 Heartbleed 漏洞攻击，成功的获得了预期的数据，并在指导书的帮助下完成了漏洞的修复；对 Crypto_Hash 哈希加密算法有了一定的认识，熟悉了单向散列函数和消息认证码，对 Crypto_Hash 有了更深层次的了解。

除了学到的安全内容之外，我也学会了如何简单的使用 LINUX 系统，掌握了一些基本的命令和常识，对以后的关于 LINUX 课程的学习有一定的帮助。同时，我也学会了如何在网上进行自主学习，对我的自主学习能力有了一定的提升。

当然，此次实验也暴露了一些问题。一是实验指导书为纯英文，英语底子薄使得我做起实验来十分费劲，很多地方需要通过猜测进行实验，导致我对实验的理解没有上升到应有的高度。二是编程能力欠缺，尤其是在 LINUX 系统下的编程，实验最后的编程没有能很好的完成。

这个实验是一个开始，对于信息安全专业来说，之后会有更多这样的实验给我们。这是一个挑战，也是一个机遇。我们更需要通过此次实验不断勉励自己，不断进步。