中南大學

网络安全
网上学习实验报告

姓　　名：杨宗元

班　　级：信息安全 1402 班

学　　号：0906140225

指导老师：王伟平

时　　间：2016 年 12 月 18 日

实验二　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。

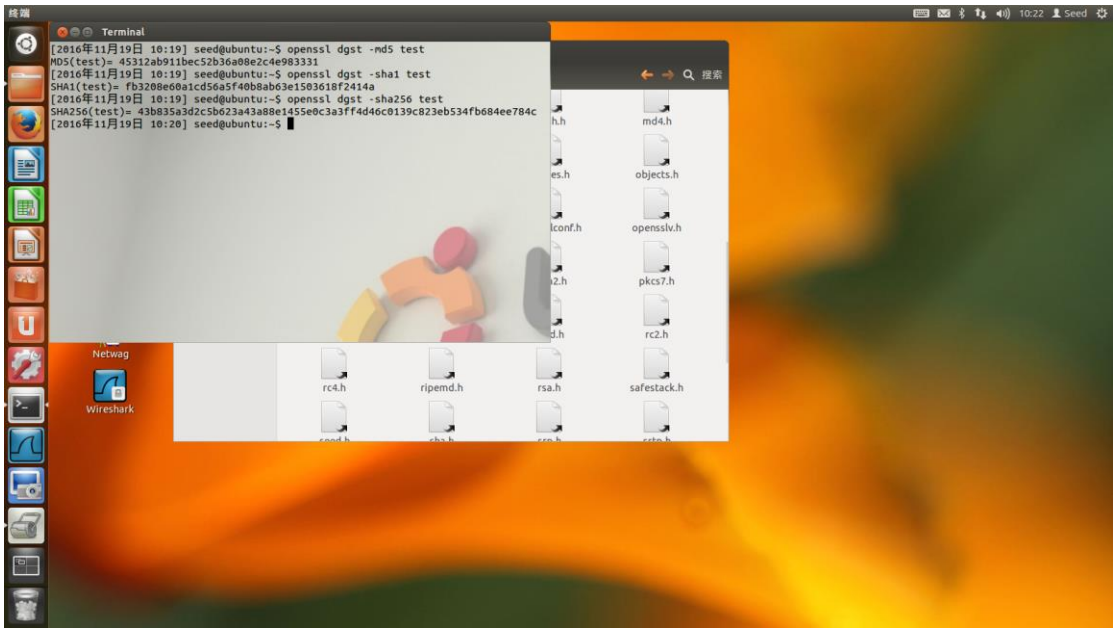
二. 实验环境及过程

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。

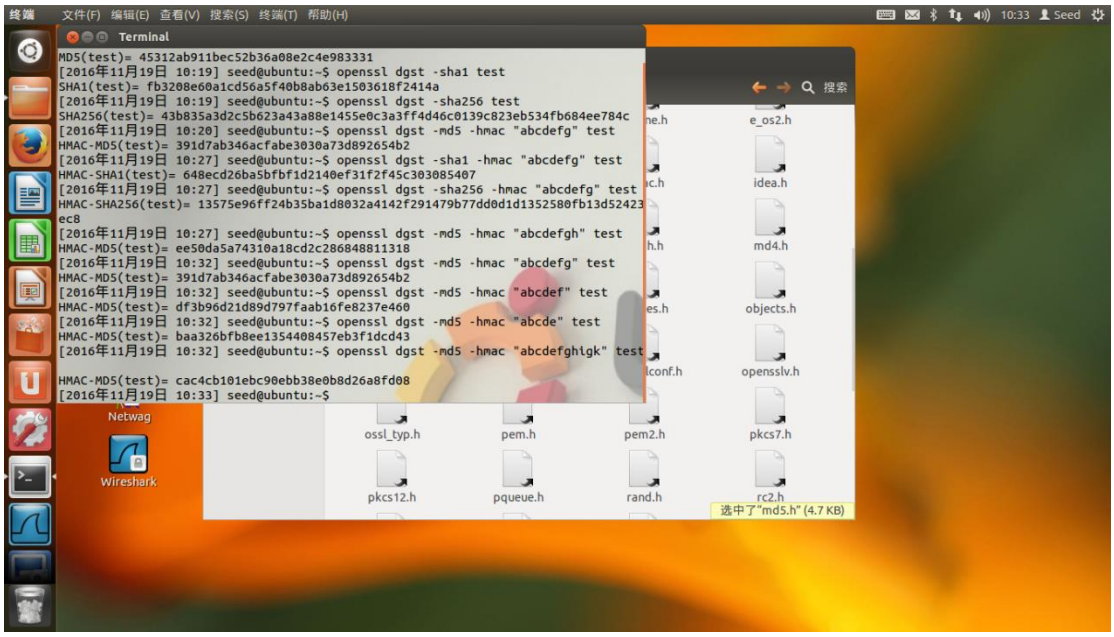
三. 实验结果

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

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

经过这几天苦心钻研，我觉得网络安全是一门很有趣的学科，它很好的发散了我们的思维，使思维更开阔，让个人的自主学习能力有了很大的飞跃，与此同时，网上学习实验也很好的锻炼了同学之间配合与协作，有很多不懂的地方可以一起钻研。程序的调试的时候常会出现许多问题，同学之间相互帮忙解决处理问题就会比较快。而在运行程序的过程中耐心也非常重要，常常会出现这样或者那样的小问题，

又很难找出来，需要的是我们的细心以及耐心去一一克服这些难题。虽然上了一学期的网络安全课程，但是真正运行来，还是有很大差距的，理论和动手之间的确有很大不同，总之很感谢这次的网上学习和学长的悉心指导，让我学到了许多以前课堂上都很难学到的知识，实践真的非常重要。在这次的网上学习中我提升了自己的实际动手能力，获益匪浅，很感谢这次的经验，为我以后打下了坚实的基础。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。起初做实验时，遇到了许多的问题，

如定义、公有函数怎么去实现所要的结果等一系列的问题，刚开始觉得有点棘手，很多问题搞不懂，不过经过和同组同学的认真讨论以及仔细的阅读教材和相关参考文献，渐渐认识到问题本质，进而将问题一一击破解决，将课程设计比较成功的完成了。但在我的整个系统整体上功能有些不太健全，自己感觉系统有点冗长，部分程序需精简，而且界面也不太美观，没有设计一些美观的板块，还有很多不足和需要改进的地方。