中南大學

CENTRAL SOUTH

网络安全课后实验

Seed project 心脏滴血

学　　院：　信息科学与工程学院

班　　级：　信息安全 1401

指导老师：　王伟平

姓　　名：　苏伟

完成时间：　2016 年 11 月

目录

第一章 褚论

1.1 实验背景

2014 年 4 月 8 日，互联网上曝出了严重一个漏洞称为 Heartbleed，该漏洞由安全公司 Codenomicon 和谷歌安全工程师发现。 Heartbleed 漏洞，造成许任何人在互联网上阅读系统的内存保护脆弱的 OpenSSL 的软件版本。 这种妥协密钥用于识别服务提供者和加密流量,用户名和密码的和实际的内容。 这允许攻击者窃听通信、窃取数据直接从服务和用户和模拟服务和用户。

在其披露时，约有 17%或五十万通过认证机构认证的互联网安全网络服务器被认为容易受到攻击。电子前哨基金会，Ars Technica，和布鲁斯·施奈尔都认为心脏出血漏洞是“灾难性的”。

漏洞让特定版本的 openSSL 成为无需钥匙即可开启的“废锁”，入侵者每次可以翻检户主的 64K 信息，只要有足够的耐心和时间，就可以翻检足够多的数据，拼凑出户主的银行密码、私信等敏感数据。

1.2 实验意义

这个实验的目的是让学生了解这个漏洞是多么严重，如何攻击的工作，以及如何解决这个问题。受影响的 OpenSSL 版本范围从 1.0.1 到 1.0.1f。作为初次进行模拟的攻击实验，这次选取较为简单的攻击还是很有意义的

第二章　　漏洞分析

Heartbleed 漏洞，这项严重缺陷(CVE-2014-0160)的产生是由于未能在memcpy()调用受害用户输入内容作为长度参数之前正确进行边界检查。攻击者可以追踪 OpenSSL 所分配的 64KB 缓存、将超出必要范围的字节信息复制到缓存当中再返回缓存内容，这样一来受害者的内存内容就会以每次 64KB 的速度进行泄露。通过读取网络服务器内存，攻击者可以访问敏感数据，从而危及服务器及用户的安全。敏感的安全数据，如服务器的专用主密钥，可使攻击者在服务器和客户端未使用完全正向保密时，通过被动中间人攻击解密当前的或已存储的传输数据，或在通信方使用完全正向保密的情况下，发动主动中间人攻击。攻击者无法控制服务器返回的数据，因为服务器会响应随机的内存块。

漏洞还可能暴露其他用户的敏感请求和响应，包括用户任何形式的 POST 请求数据，会话 cookie 和密码，这能使攻击者可以劫持其他用户的服务身份。

第三章　　实验过程

3.1 实验一