中南大学

《SEED PROJECT》
实验报告

学生姓名 韩军

指导教师 王伟平

学　　院 信息科学与工程

专业班级 信息安全 1401

完成时间 2016.12

实验一　Heartbleed Attack Lab

一、实验原理

Heartbleed bug (CVE-2014-0160)是旧版本的 Openssl 库中一个的一个漏洞。利用这个漏洞，攻击者可以从服务器里窃取一部分随机数据。这个漏洞主要是源于 Openssl 设计的协议继承了 Heartbeat 协议，使用 SSL/TLS 来保持连接的实时性、保活性。

Heartbeat 协议的主要工作原理如下：

Heartbeat 协议使用两种数据包来进行连接：HeartbeatRequest 数据包和 HeartbeatResponse 数据包。当客户端需要煜服务器建立时，客户端首先会发送 HeartbeatRequest 数据包到服务器，该数据包会包含一些信息。当服务器收到 HeartbeatRequest 数据包，会返回一个 HeartbeatResponse 数据包，该数据包中会有一份 HeartbeatRequest 数据包中信息的复制样本。这样，双方就确立了连接。但是在这个协议中，有一个脆弱点，就是实际上客户端是可以设定信息长度的。这样的话，攻击者就可以设定信息长度大于它实际长度，这样的话，服务器在返回数据包时，由于实际上信息不够，它会将自身保存的后面的信息拼接在客户端发送过来的信息后面。这样我们就可以拿到服务器的数据。但是实际上这是一个随机的过程，因为服务器返回的信息取决于客户端发送信息存储的位置。所以想得到关键信息，有时候需要一点运气和多几次的尝试。

原理示意图如下：

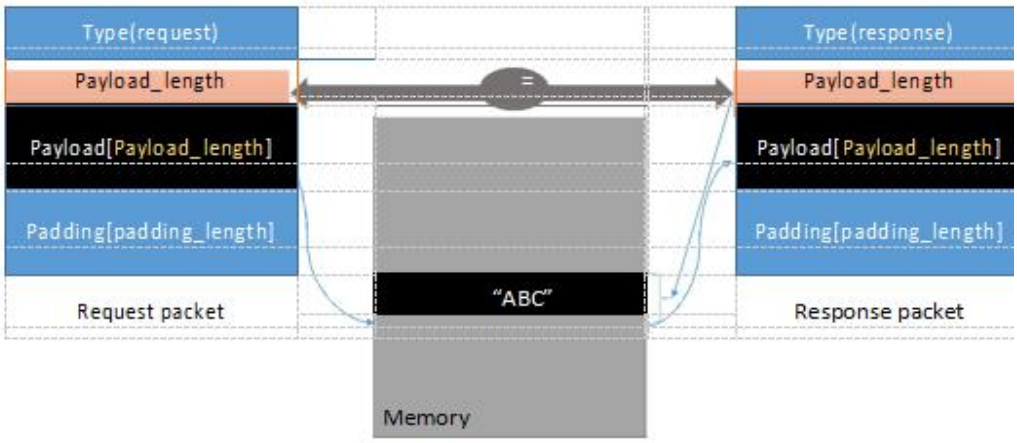


Figure 2: The Benign Heartbeat Communication

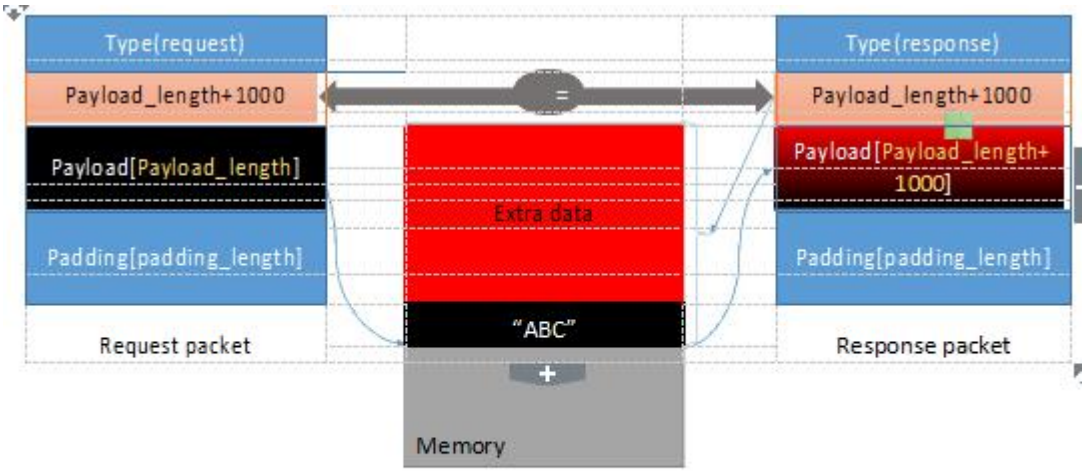


Figure 3: The Heartbleed Attack Communication

二、实验过程

Task1：

首先要按照指导进行如下操作：

访问您的浏览器 https://www.heartbleedlabelgg.com。登录网站管理员。（用户名：admin 密码：seedelgg；）增加朋友。（去更多->点击波比->添加朋友），然后发送私人消息。

在您已经做了足够的互动作为合法用户，你可以发动攻击，看看你可以从受害者服务器上得到什么信息。编写程序从零开始推出 Heartbleed 攻击是不容易的，因为它需要的心跳协议底层的知识。幸运的是，其他人已经写了攻击代码。因此，我们将使用现有的代码来获得在 Heartbleed 攻击的第一手经验。我们使用的代码称为 attack.py，原本是 Jared Stafford 写的。我们对教育目的的代码做了一些小的修改。您可以从实验室的网站上下载代码，更改其权限，所以该文件是可执行的。然后，您可以运行攻击代码如下：

$ / attack.py www.heartbleedlabelgg.com。

您可能需要多次运行攻击代码以获取有用的数据。尝试，看看是否可以从目标服务器获取以下信息。

用户名和密码。

用户活动（用户所做的）。私人信息的确切内容。

Task2：

在这个任务中，学生将比较良性包和被攻击者发送的代码发送的恶意数据包的去发现 Heartbleed 漏洞的根本原因。Heartbleed 攻击是基于 heartbeatrequest。这个请求只是向服务器发送一些数据，服务器将将数据复制到它的响应数据包中，所以所有的数据都被响应了。

在正常情况下，假设请求包括 3 个字节的数据“作业”，所以长度字段有一个值 3。服务器将将数据放在内存中，并从数据的开始复制 3 个字节到它的响应数据包。在攻击场景中，请求可能包含 3 个字节的数据，但长度字段可以说 1003。当服务器构造它的响应数据包时，它从数据的开始（即“美国广播公司”）复制，但它拷贝 1003 个字节，而不是 3 个字节。这些额外的 1000 种类型显然不来自请求数据包，它们来自服务器的私有内存，它们可能包含其他用户的信息、密钥、密码等。

在这项任务中，我们将改变请求数据包的长度字段来观察结果。

你的任务是用不同的有效载荷长度的值来播放攻击程序，并回答以下问题：

问题 2.1：随着长度变量的减少，你会观察到什么样的差异？

问题 2.2：为可变长度的减小，有输入长度可变的边界值。在或低于该边界，heartbeat 将接收一个响应数据包，而不附加任何额外的数据（这意味着该请求是良性的）。请发现边界长度。您可能需要尝试许多不同的长度值，直到 Web 服务器发送回没有额外的数据的答复

Task3：

修复 Heartbleed 漏洞，最好的办法是更新到最新版本的 OpenSSL 库。这可以实现使用以下命令。

```
#sudo apt-getupdate
#sudoapt-getupgrae
```

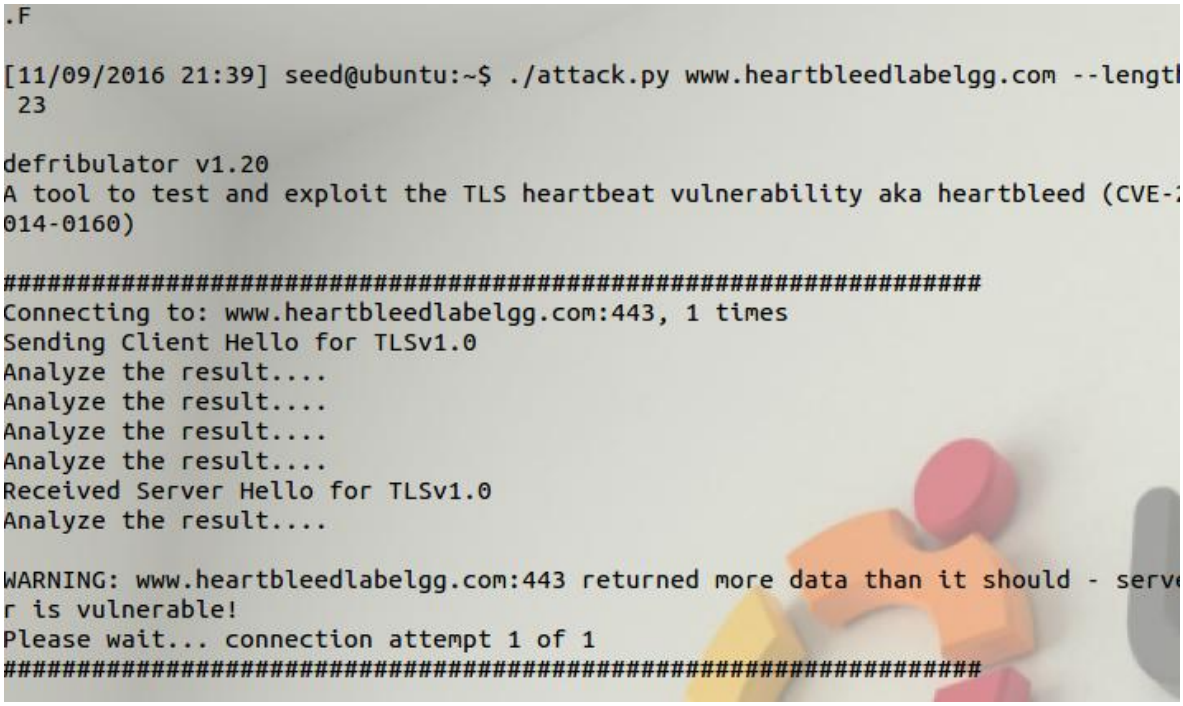
应该指出的是，一旦它被更新，很难再回到有漏洞的版本。因此，请确保您在做更新之前完成了以前的任务。您还可以在更新之前对您的虚拟机进行快照。

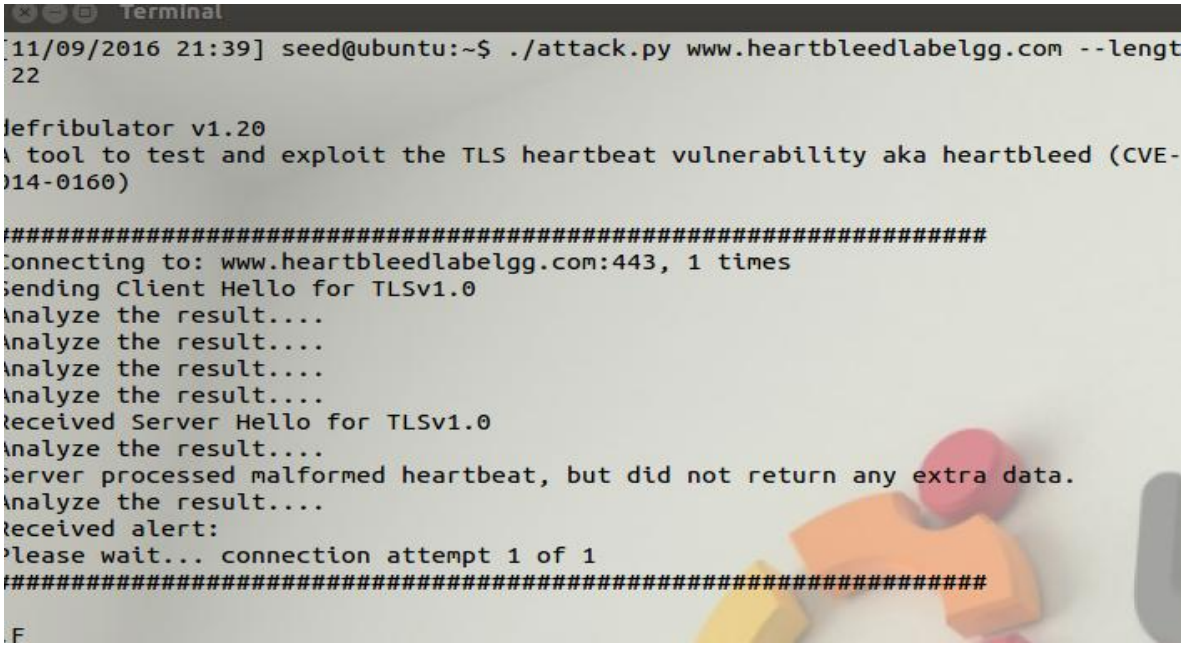
三、实验结果以及讨论

按照实验指导完成 Task1 之后，下载脚本到计算机并运行之后，就可以观察到

成功捕获到了用户名以及密码。

在 task2 中，设置长度为 22 和 23 时返回消息分别如下所示：





对于问题 2.1，由观察的结构可以得知，边界值为 22.
对于问题 2.2.，当缩短指定的长度时，返回的数据包长度也会相应的缩短。在我看来，解决这个漏洞可以让 heartrequest 的数据包不能被更改，即自动根据信息来由服务器来计算长度，这样的话，服务器就不会返回另外的数据。还可以让服务器进行校验，当长度不一致时，取信息的长度做回返回的数据长度值。在我看来，这样应该可以解决问题。当然，在实际中可能会有技术限制等别的问题，所以这是我的考虑。参考了资料觉得应该是可行的。
在 Task3，更新更新到最新版本的 OpenSSL 库时，指定数据包的长度就会不起作用了，补丁已经打好了。

四、实验思考

总体上来说，本次实验并不算难，没有太多引申发散思考，主要是按照以前已有的攻击步骤来实施，而且也不要自己来写攻击代码。

我在网上查阅以后，受影响的主要是以下两个 SSL 版本：

- OpenSSL 1.0.2-beta
- OpenSSL 1.0.1 - OpenSSL 1.0.1f

虽然这个漏洞早就已经得到了安全补丁，但是我们可以从中吸一些经验。缺少检验的标准往往会存在一些可以利用的漏洞，比如曾经的“PING OF DEATH“攻击，就是利用了 ICMP 类型的数据包没有进行对包内数据长度进行核验的漏洞，进行 DOS 攻击。所以检验是很重要的一类安全属性。

最后要谢谢老师和学长们的指导。谢谢！