中南大学

Heartbleed 攻击

实验报告

学生姓名 刘晓悦

专业班级 信安 1401

学　　号 0906140118

学　　院 信息科学与工程学院

指导教师 王伟平

实验时间 2016 年 12 月

Heartbleed 攻击实验

1 概述

Heartbleed 错误是 OpenSSL 库中的一个严重的实现缺陷，它启用攻击者从受害者服务器的内存窃取数据。被盗数据的内容取决于什么是在服务器的内存中。它可以潜在地包含私钥，TLS 会话密钥，用户名称，密码，信用卡等。漏洞是在 Heartbeat 协议的实现，其由 SSL / TLS 用于保持连接活动。本实验的目的是让学生了解这个漏洞是多么严重，如何攻击工作，以及如何解决这个问题。

2 实验室环境

在本实验中，我们需要设置两个虚拟机：一个称为攻击者计算机，另一个称为受害服务器。

我们使用预构建的 SEEDUbuntu12.04 VM。 VM 需要使用 NAT-网络适配器网络设置。这可以通过转到 VM 设置，选择网络，然后单击适配器来完成标签将适配器切换到 NAT-Network。确保两个虚拟机在同一 NAT 网络上。此攻击中使用的网站可以是使用 SSL / TLS 的任何 HTTPS 网站。然而，因为它是非法攻击一个真实的网站，我们在我们的 VM 中设置了一个网站，并自己进行攻击 VM。我们使用一个名为 ELGG 的开源社交网络应用程序，并将其托管在以下 URL 中：

https://www.heartbleedlabelgg.com。

我们需要修改攻击者计算机上的/ etc / hosts 文件，将服务器名称映射到 IP 地址的服务器 VM。搜索/ etc / hosts 中的以下行，并替换 IP 地址 127.0.0.1 与托管 ELGG 应用程序的服务器 VM 的实际 IP 地址。

127.0.0.1 www.heartbleedlabelgg.com

3 实验室任务

心跳协议由两种消息类型组成：HeartbeatRequest 包和 HeartbeatResponse 包。客户向服务器发送 HeartbeatRequest 包。当服务器接收到它时，它发送回的副本在 HeartbeatResponse 包中接收到的消息。目标是保持连接活着。

3.1 任务 1：启动 Heartbleed 攻击。

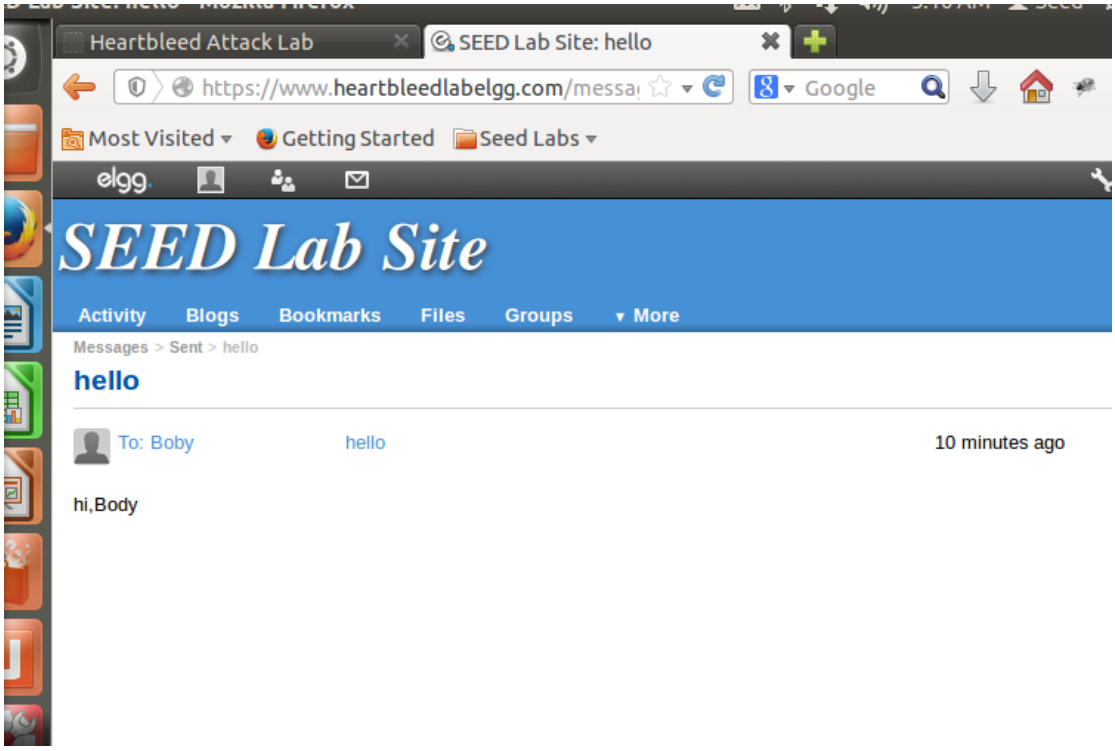
在这个任务中，学生将在我们的社交网站上启动 Heartbleed 攻击，看看是什么样的可以实现损坏。 Heartbleed 攻击的实际伤害取决于什么样的信息存储在服务器存储器中。如果服务器上没有太多活动，您将无法访问窃取有用数据。因此，我们需要作为合法用户与 Web 服务器进行交互。让我们做它管理员，并执行以下操作：

•从浏览器访问 https://www.heartbleedlabelgg.com。

•以站点管理员身份登录。 （用户名：admin;密码：seedelgg）

•将 Boby 添加为朋友。 （转到更多 - >成员，然后单击 Boby - >添加好友）

•向 Boby 发送私人消息。



然后可以运行攻击代码如下：

$ ./attack.py www.heartbleedlabelgg.com

Listing 1: Process the Heartbeat request packet and generate the response packet

```
/* Allocate memory for the response, size is 1 byte
 * message type, plus 2 bytes payload length, plus
 * payload, plus padding
 */

unsigned int payload;
unsigned int padding = 16; /* Use minimum padding */

// Read from type field first
hbtype = *p++; /* After this instruction, the pointer
              * p will point to the payload_length field *.

// Read from the payload_length field
// from the request packet
n2s(p, payload); /* Function n2s(p, payload) reads 16 bits
              * from pointer p and store the value
              * in the INT variable "payload". */


pl=p; // pl points to the beginning of the payload content

if (hbtype == TLS1_HB_REQUEST)
{
    unsigned char *buffer, *bp;
    int r;

    /* Allocate memory for the response, size is 1 byte
     * message type, plus 2 bytes payload length, plus
     * payload, plus padding
     */

    buffer = OPENSSL_malloc(1 + 2 + payload + padding);
    bp = buffer;

    // Enter response type, length and copy payload
    *bp++ = TLS1_HB_RESPONSE;
    s2n(payload, bp);

    // copy payload
    memcpy(bp, pl, payload); /* pl is the pointer which
                        * points to the beginning
                    * of the payload content */

    bp += payload;

    // Random padding
    RAND_pseudo_bytes(bp, padding);

    // this function will copy the 3+payload+padding bytes
    // from the buffer and put them into the heartbeat response
    // packet to send back to the request client side.
    OPENSSL_free(buffer);

    r = ssl3_write_bytes(s, TLS1_RT_HEARTBEAT, buffer,
        3 + payload + padding);
}
```

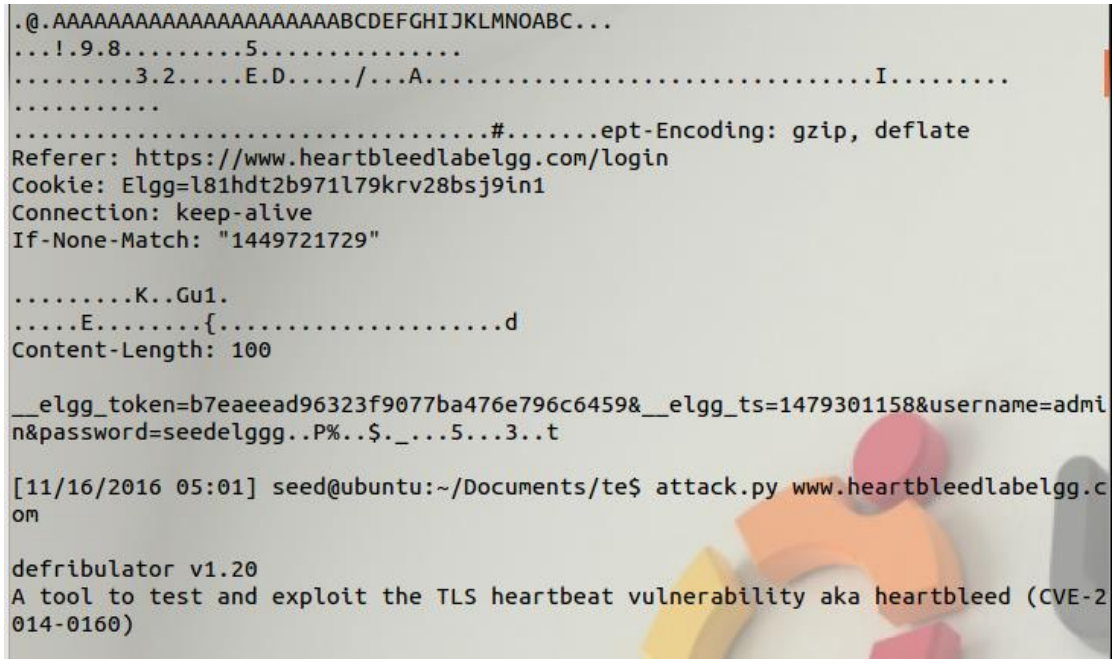
您可能需要多次运行攻击代码以获取有用的数据。试着看看你能不能得到从目标服务器获取以下信息。

•用户名和密码。

•用户的活动（用户做了什么）。

•私人消息的确切内容。

对于你从 Heartbleed 攻击中窃取的每一个秘密，你需要显示屏幕转储证明和解释你是如何做的攻击，以及你的观察是什么。



3.2 任务 2：查找 Heartbleed 漏洞的原因

在这个任务中，学生将比较良性数据包的结果和发送的恶意数据包攻击者代码来找出 Heartbleed 漏洞的根本原因。

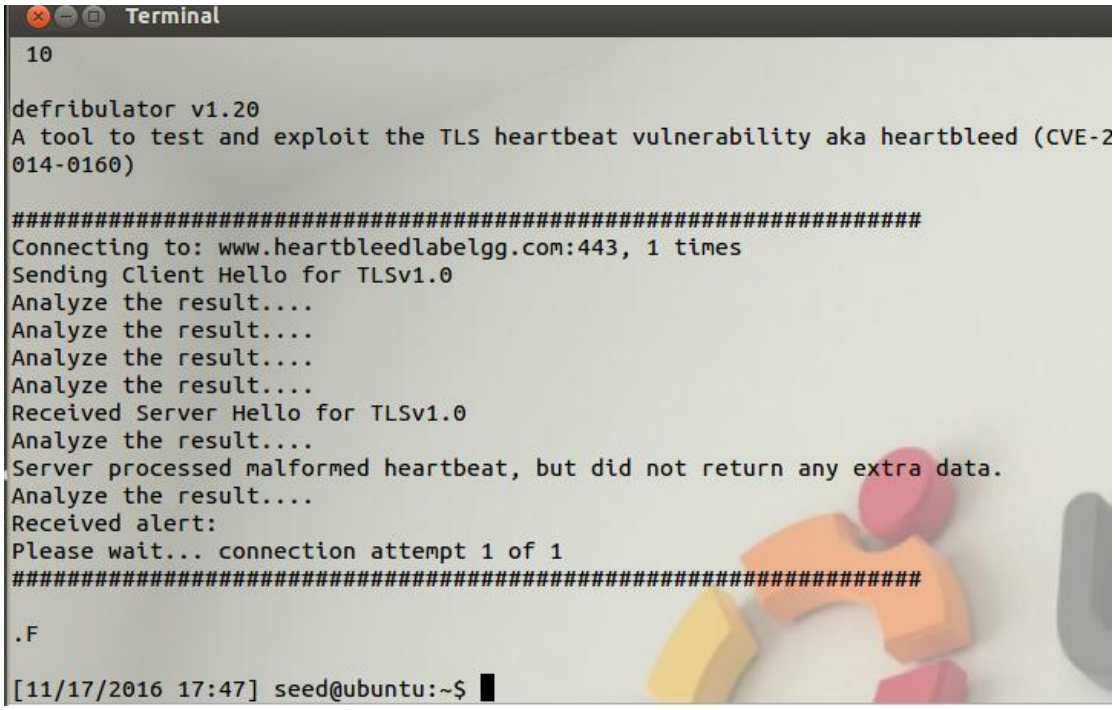
Heartbleed 攻击基于 Heartbeat 请求。这个请求只是发送一些数据到服务器，并且服务器将数据复制到其响应包，因此所有数据被回送。在正常情况下，

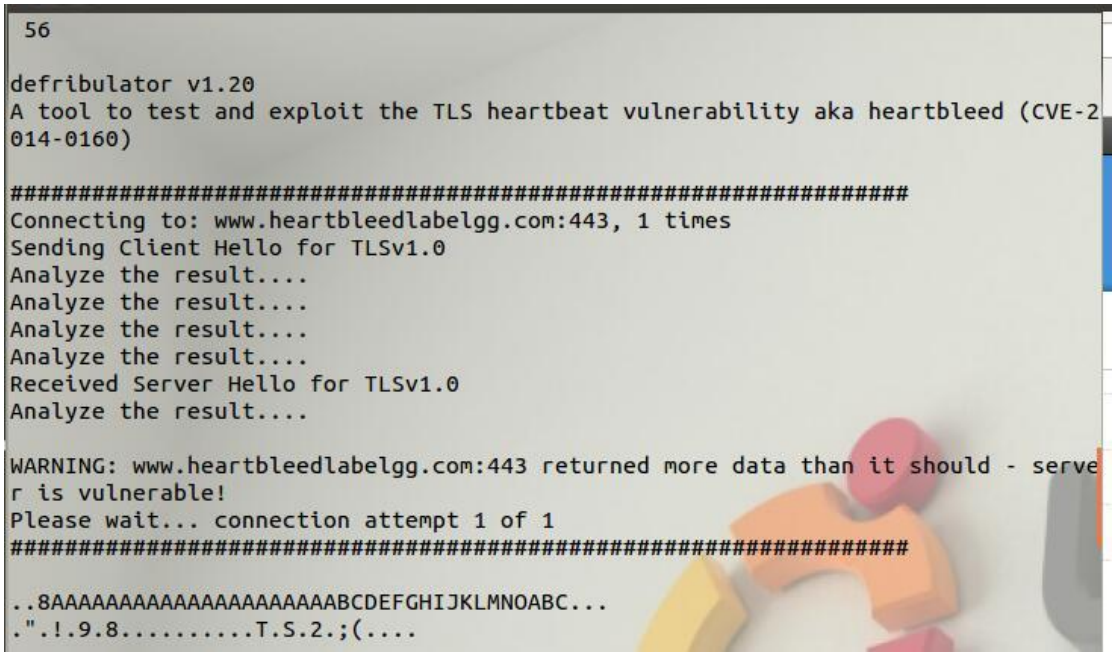
假设请求包括 3 字节的数据“ABC”，因此长度字段具有值 3.服务器将
将数据放置在存储器中，并且从数据的开始将 3 个字节复制到其响应分组。在里面
攻击情形，请求可能包含 3 个字节的数据，但长度字段可能表示为 1003.当服务器
构造其响应分组，它从数据的开始（即“ABC”）复制，但是它复制 1003 字节，而不是 3 个字节。这些额外的 1000 个类型显然不是来自请求包;他们来自
服务器的私人内存，它们可能包含其他用户的信息，密钥，密码等。
在这个任务中，我们将使用请求的长度字段。首先，让我们来了解心跳
响应包从图 2 构建。当 Heartbeat 请求包到来时，服务器将解析
分组以获得有效载荷和有效载荷长度值（在图 2 中突出显示）。这里，
有效负载只是一个 3 字节的字符串“ABC”，Payload 长度值正好是 3.服务器程序将盲目地从请求分组中取出这个长度值。然后它通过指向构建响应数据包

存储器存储“ABC”并将有效负载长度字节复制到响应有效载荷。这样，
响应包将包含一个 3 字节的字符串“ABC”。
我们可以启动 HeartBleed 攻击，如图 3 所示。我们保持相同的有效负载（3 字节），但将 Payload 长度字段设置为 1003.服务器将再次盲占该有效负载长度
值构建响应包。这一次，服务器程序将指向字符串“ABC”和
将 1003 字节从存储器复制到作为有效载荷的响应分组。除了字符串“ABC”，额外
1000 字节被复制到响应包中，其可以是来自存储器的任何东西，诸如秘密
活动，日志信息，密码等。
我们的攻击代码允许你使用不同的有效载荷长度值。默认情况下，值为
设置为相当大的一个（0x4000），但是您可以使用命令选项“-l”（字母 ell）减小大小，
或“ - length”，如以下示例所示：

```
$。/ attack.py www.heartbleedlabelgg.com -l 0x015B
$。/ attack.py www.heartbleedlabelgg.com --length 83
```

你可能需要尝试许多不同的长度值，直到 Web 服务器发回回复，没有额外的数据。至帮助你这样，当返回的字节数小于预期的长度，程序将打印“服务器处理的畸形心跳，但没有返回任何额外数据”。


Terminal
10
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2
014-0160)
Connecting to: www.heartbleedlabelgg.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....
Server processed malformed heartbeat, but did not return any extra data.
Analyze the result....
Received alert:
Please wait... connection attempt 1 of 1
.F
[11/17/2016 17:47] seed@ubuntu:~$


56
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2
014-0160)
Connecting to: www.heartbleedlabelgg.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....
WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - serve
r is vulnerable!
Please wait... connection attempt 1 of 1
..8AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
.".!.9.8..........T.S.2.;(....