中南大學

CENTRAL SOUTH UNIVERSITY

网 络 安 全 实 验 报 告

学生姓名 夏该致

专业班级 信息安全 1401

学　　号 0906140109

学　　院 信息科学与工程学院

指导教师 王伟平

实验时间 2016 年 11 月

实验一　心脏滴血

一。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。

通过读取网络服务器内存，攻击者可以访问敏感数据，从而危及服务器及用户的安全。敏感的安全数据，如服务器的专用主密钥，可使攻击者在服务器和客户端未使用完全正向保密时，通过被动中间人攻击解密当前的或已存储的传输数据，或在通信方使用完全正向保密的情况下，发动主动中间人攻击。攻击者无法控制服务器返回的数据，因为服务器会响应随机的内存块。[8]

漏洞还可能暴露其他用户的敏感请求和响应，包括用户任何形式的 POST 请求数据，会话 cookie 和密码，这能使攻击者可以劫持其他用户的服务身份。在其披露时，约有 17%或五十万通过认证机构认证的互联网安全网络服务器被认为容易受到攻击。电子前哨基金会，Ars Technica，和布鲁斯·施奈尔都认为心脏出血漏洞是“灾难性的”。

二。实验步骤

1. 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。

2. 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. 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。
•登录站点管理员。(用户名:admin,密码:seedelgg)
•波比添加为朋友。(去更多- >成员,然后单击波比- >添加朋友)
•发送波比私人消息。
之后你做了足够的互动为合法用户,你可以发起攻击,看看
受害者服务器的信息,你就可以出去。编写的程序来启动 Heartbleed 攻击
划痕是不容易的,因为它需要心跳协议的低层次的知识。幸运的是,其他
人已经写攻击代码。因此,我们将使用现有的代码来获得第一手资料
经验 Heartbleed 攻击。我们使用的代码称为攻击。py,最初
杰瑞德斯塔福德写的。我们做了一些小修改代码用于教育目的。你可以
从实验室的网站上下载代码,改变其许可文件是可执行的。然后您可以运行
攻击代码如下:
美元。/攻击。py www.heartbleedlabelgg.com
你可能需要多次运行攻击代码获得有用的数据。试一试,看看你是否可以得到
以下信息的目标服务器。
•用户名和密码。
•用户的活动(用户所做的)。
•私人信息的具体内容。
每一块的秘密你偷 Heartbleed 攻击,你需要显示的屏幕转储
证明和解释你如何做的攻击,以及你的观察是什么。

4. 任务 2:找到 Heartbleed 脆弱性的原因

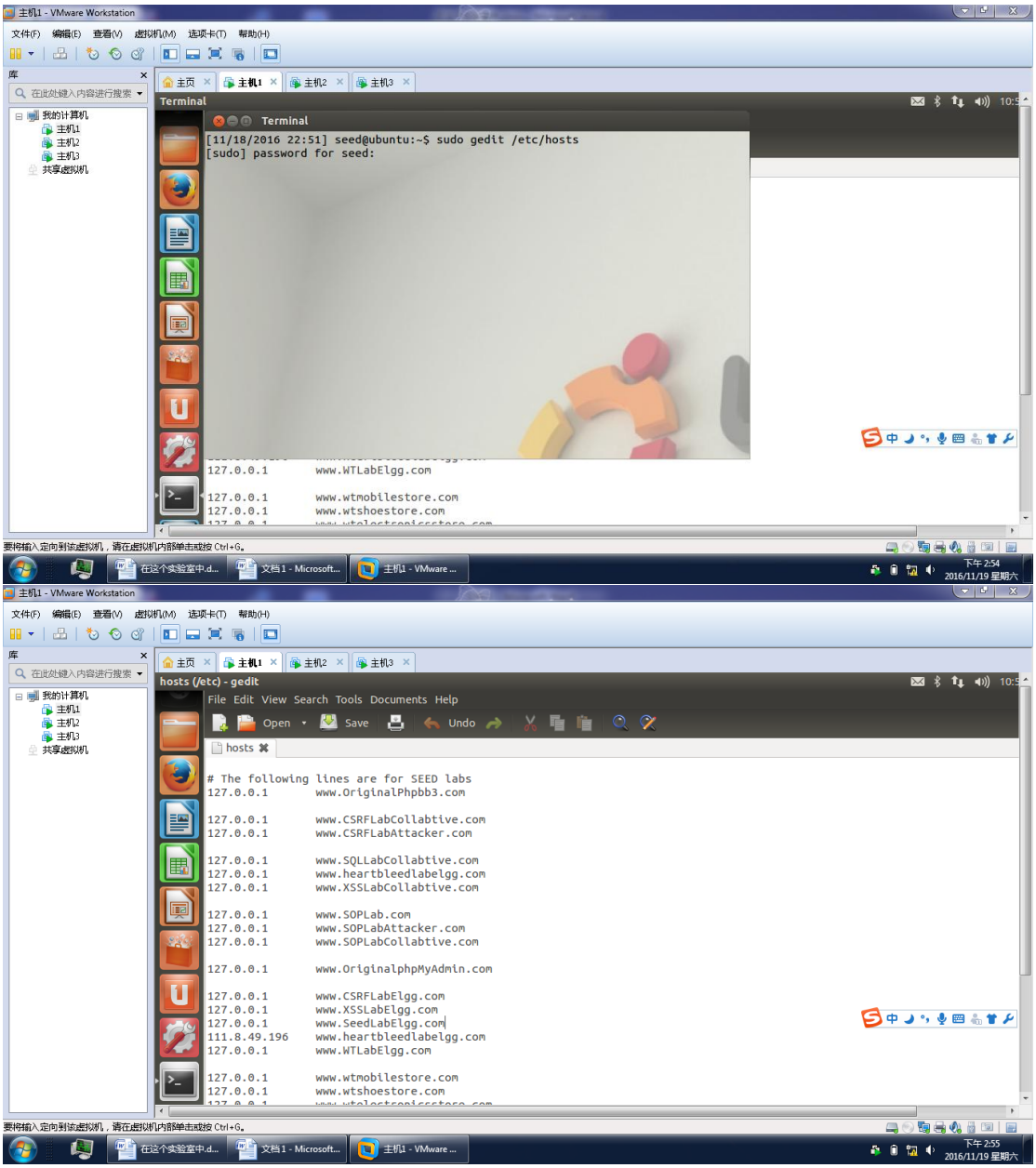
在这个任务中,学生将比较良性的结果包和恶意数据包发送的
攻击者的代码来找出 Heartbleed 脆弱性的根本原因。
Heartbleed 攻击是基于心跳请求。这仅仅请求向服务器发送一些数据,
和服务器将数据复制到响应数据包,所以所有的数据都是回荡。在正常的情况下,
假设请求包括 3 字节的数据“ABC”,所以长度字段有值 3。服务器将
内存中的数据,从一开始就 3 个字节的数据复制到响应包。在
攻击场景,请求可能包含 3 个字节的数据,但长度字段可能会说 1003。当服务器
结构响应数据包,它从开始的数据副本(例如“ABC”),但它拷贝 1003 字节,

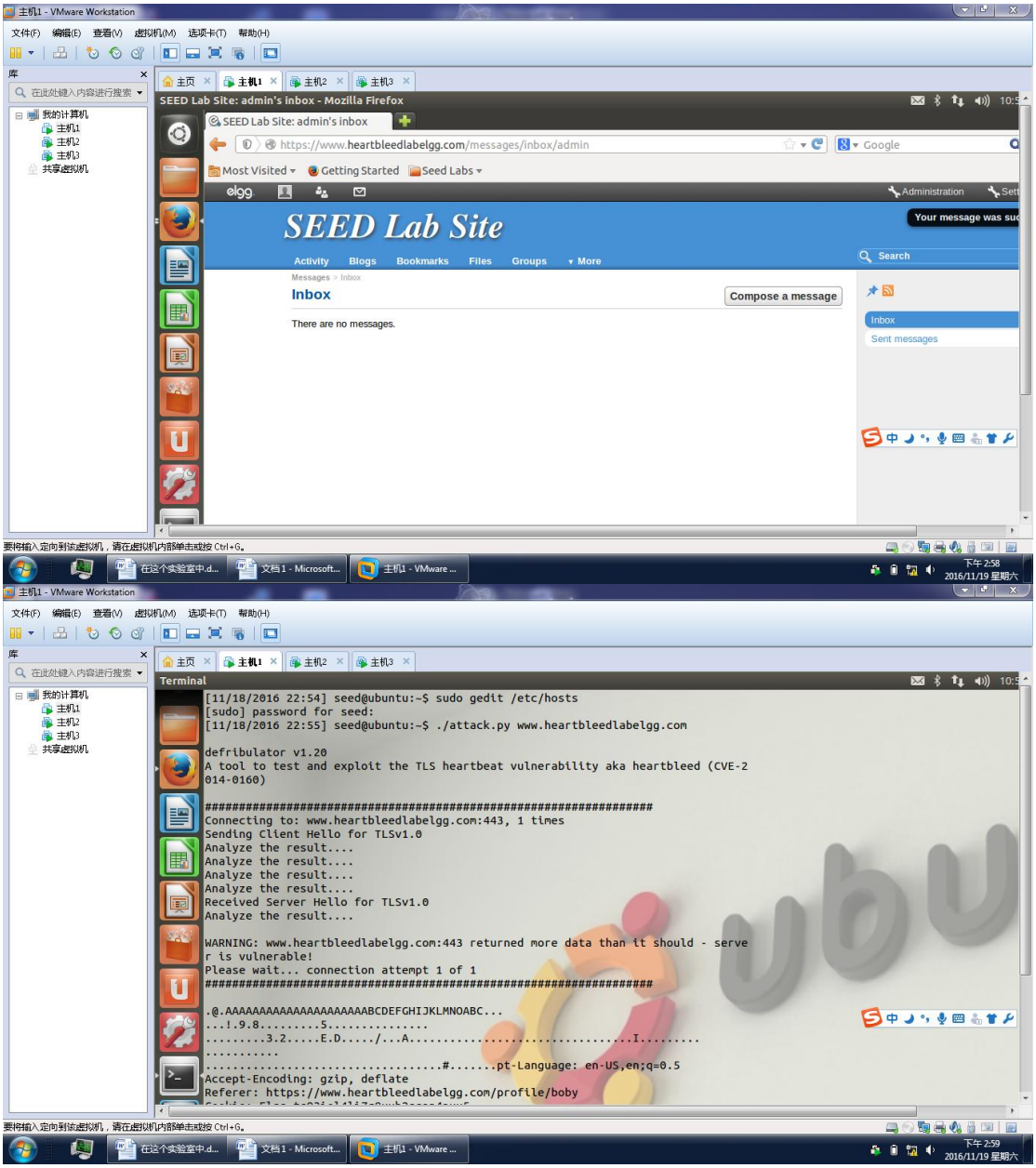
而不是 3 个字节。这些额外的 1000 种显然不来自于请求数据包;它们来自哪里
服务器的私有内存,他们可能包含其他用户的信息、密钥、密码等。
在这个任务中,我们会玩的长度字段的要求。首先,让我们了解心跳
响应数据包是由图 2。心跳请求数据包时,服务器将解析
数据包的有效载荷和载荷长度值(在图 2 中突出显示)。在这里,
载荷只有一个 3 字节的字符串“ABC”和有效载荷长度值是 3。服务器程序
盲目地将这个请求数据包的长度值。然后通过指向构建响应包

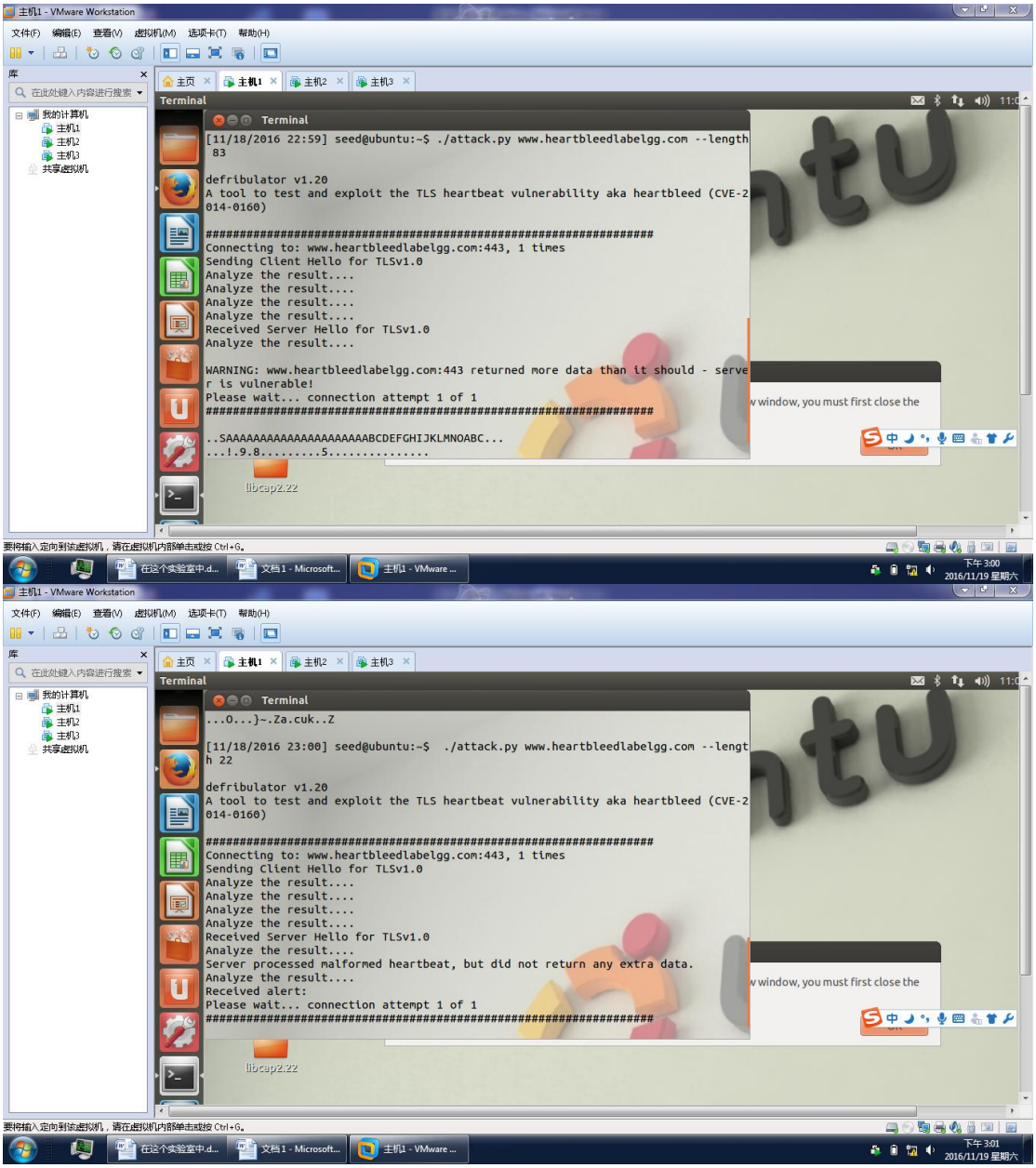
图 3:Heartbleed 攻击沟通
内存存储“ABC”,将载荷长度字节复制到响应负载。通过这种方式,
响应包将包含一个 3 字节的字符串“ABC”。
我们可以启动 HeartBleed 攻击如图 3 所示。我们保持相同的负载(3 字节),
但将载荷长度字段设置为 1003。服务器又盲目地将此载荷长度
价值在构建响应包。这一次,服务器程序将字符串“ABC”和
1003 字节的内存复制到响应数据包有效载荷。除了字符串“ABC”,额外的
1000 字节复制到响应包,它可以是任何的记忆,如秘密
活动日志信息、密码等等。
我们的攻击代码允许您玩不同的载荷长度值。默认情况下,这个值是
设置为一个相当大的一个(0 x4000),但你可以减少使用命令选项“- l”(字母 l 形)

或“长度”,下面的例子所示:
美元。/攻击。py x015b www.heartbleedlabelgg.com - l0
美元。/攻击。py www.heartbleedlabelgg.com——长度 83
你的任务是攻击程序玩不同的载荷长度值和回答下面
问题:
•问题 2.1:可变长度减少,什么样的区别你可以观察吗?
•问题 2.2:可变长度减少,有一个边界值为输入变量的长度。
在或低于边界,心跳不附带的查询将会收到一个响应数据包
任何额外的数据(这意味着请求良性)。请发现边界长度。你可能需要
尝试不同的长度值到 web 服务器发送回答复没有额外的数据。来
帮你解决这个问题,当返回的字节数量小于预期的长度,程序
将打印”服务器处理心跳畸形,但没有回复呢
任何额外的数据。”
3.3 任务 3:对策和 Bug 修复
修复 Heartbleed 脆弱,最好的方法是 OpenSSL 库更新到最新版本。
这可以通过使用下面的命令。应该注意的是,一旦它被更新时,很难
回到脆弱的版本。因此,确保你已经完成了前面的任务之前做的
更新。你可以把虚拟机的快照更新。
sudo apt-get 更新
sudo apt-get 升级

三。实验结果


主机1 - VMware Workstation
Terminal
[11/18/2016 22:51] seed@ubuntu:~$ sudo gedit /etc/hosts
[sudo] password for seed:
127.0.0.1 www.WTLabElgg.com
127.0.0.1 www.wtmobilestore.com
127.0.0.1 www.wtshoestore.com
hosts (/etc) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
hosts
The following lines are for SEED labs
127.0.0.1 www.OriginalPhpbb3.com
127.0.0.1 www.CSRFLabCollabtive.com
127.0.0.1 www.CSRFLabAttacker.com
127.0.0.1 www.SQLLabCollabtive.com
127.0.0.1 www.heartbleedlabelgg.com
127.0.0.1 www.XSSLabCollabtive.com
127.0.0.1 www.SOPLab.com
127.0.0.1 www.SOPLabAttacker.com
127.0.0.1 www.SOPLabCollabtive.com
127.0.0.1 www.OriginalphpMyAdmin.com
127.0.0.1 www.CSRFLabElgg.com
127.0.0.1 www.XSSLabElgg.com
127.0.0.1 www.SeedLabElgg.com
111.8.49.196 www.heartbleedlabelgg.com
127.0.0.1 www.WTLabElgg.com
127.0.0.1 www.wtmobilestore.com
127.0.0.1 www.wtshoestore.com


主机1 - VMware Workstation
SEED Lab Site: admin's inbox - Mozilla Firefox
SEED Lab Site
Inbox
There are no messages.
Compose a message
Terminal
[11/18/2016 22:54] seed@ubuntu:~$ sudo gedit /etc/hosts
[sudo] password for seed:
[11/18/2016 22:55] 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....
Received Server Hello for TLSv1.0
WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/profile/boby



四。实验心得

这一次实验对软件不太熟悉，大部分时间都花在了软件的安装上，浪费了大量时间，刚开始第一个软件死活装不上。换了 vm 才能使用，略坑。实验让我了解了心脏滴血这个漏洞攻击，增长了阅历。