COMPUTER NETWORKS SECURITY LABORATORY

LAB 5

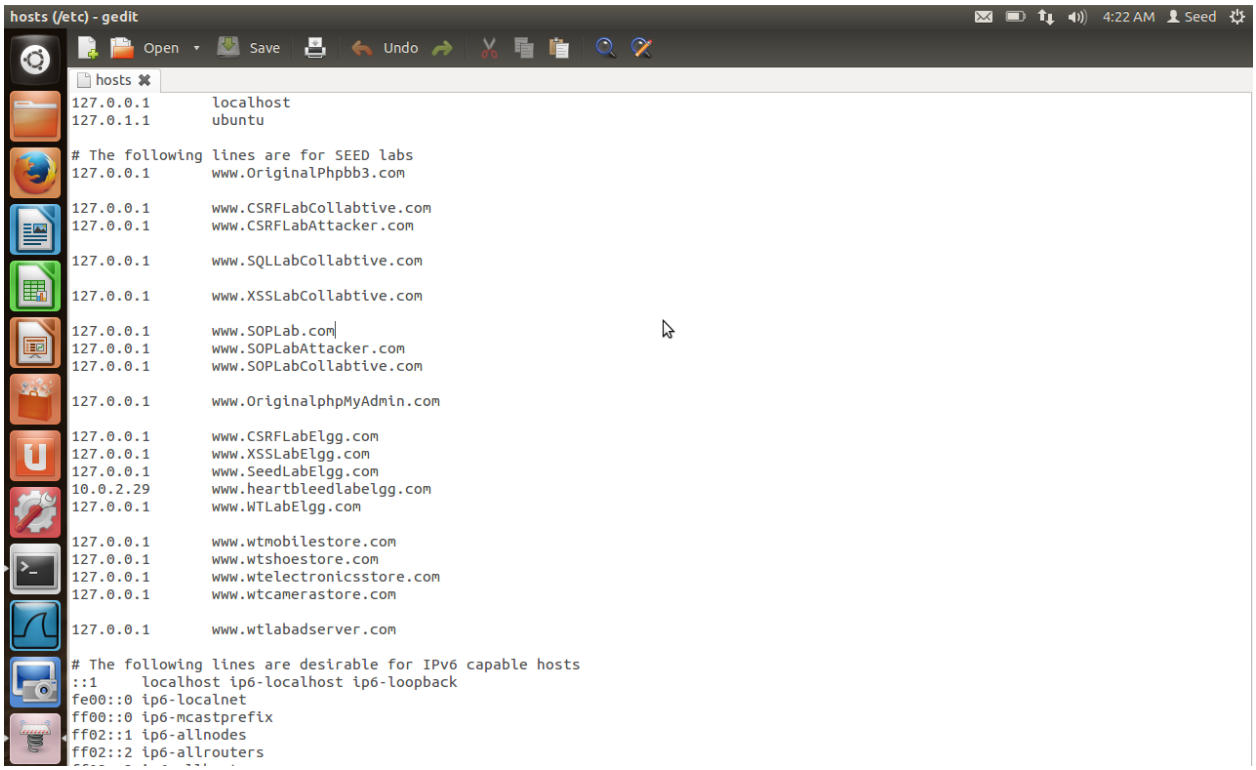
BY: RAJDEEP SENGUPTA

SRN: PES1201800144

SECTION: C

NOTE: Please find my SRN ‘PES1201800144rajdeep’ as the terminal username. Also find the description and result analysis and observation of each task in RED FONT following the screenshots for each task.

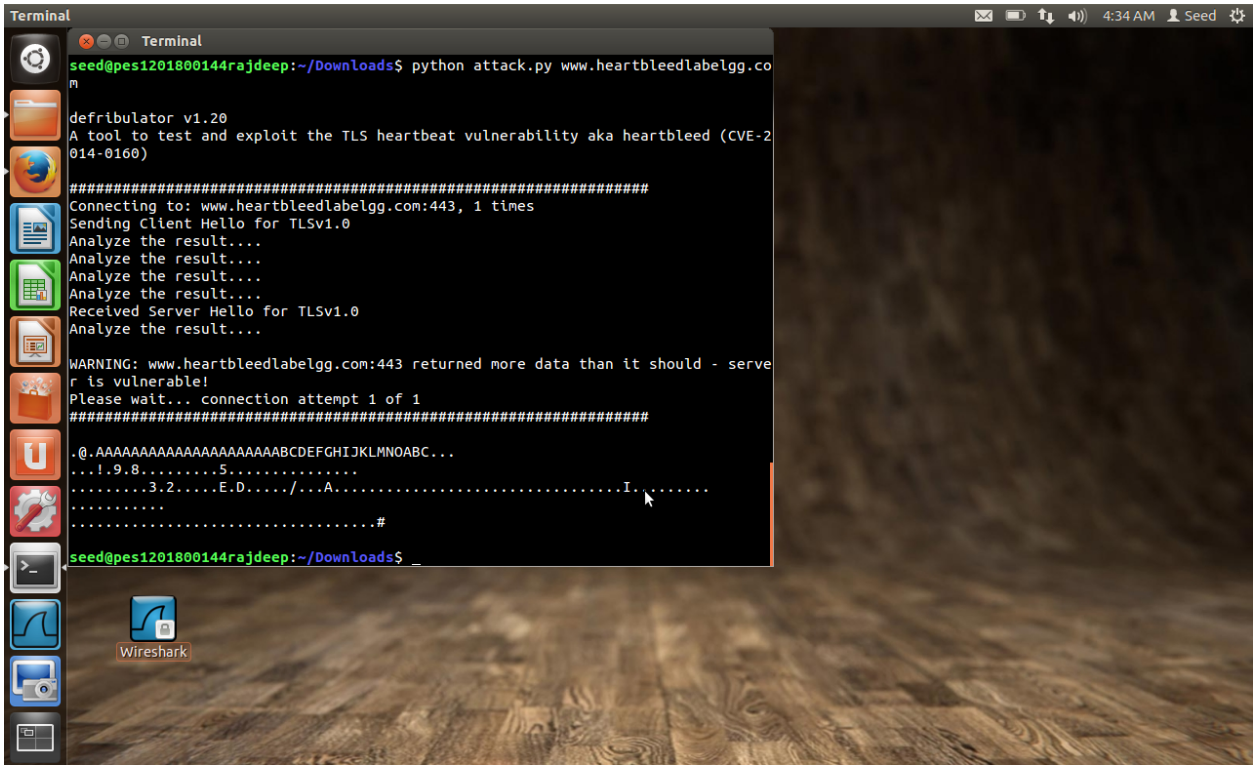
TASK 1.1: CONFIGURE THE DNS SERVER FOR ATTACKER MACHINE



Screenshot 1.1: Configuring /etc/hosts file in attacker machine

Configuring the /etc/hosts file so that whenever the attacker machine queries www.heartbleedlabelgg.com, he is directed to the apache server of 10.0.2.29(server VM).

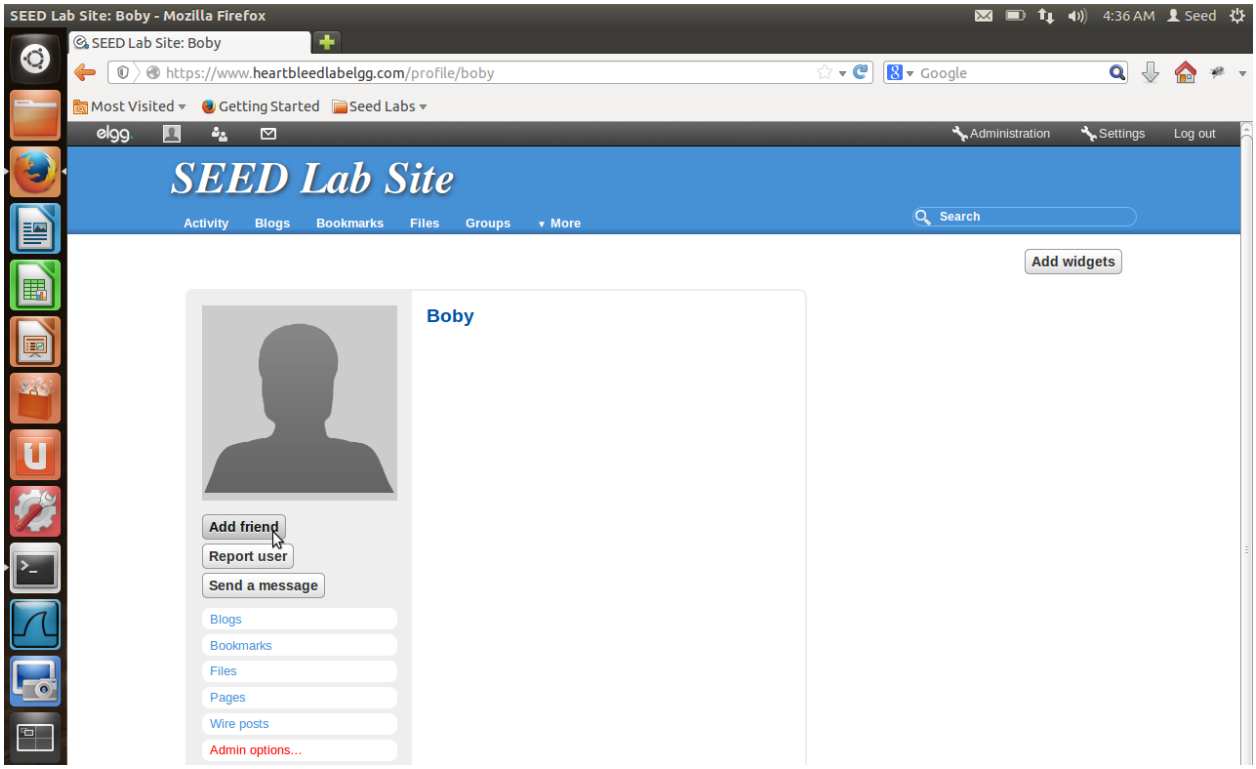
TASK 1.2: RUNNING THE ATTACK



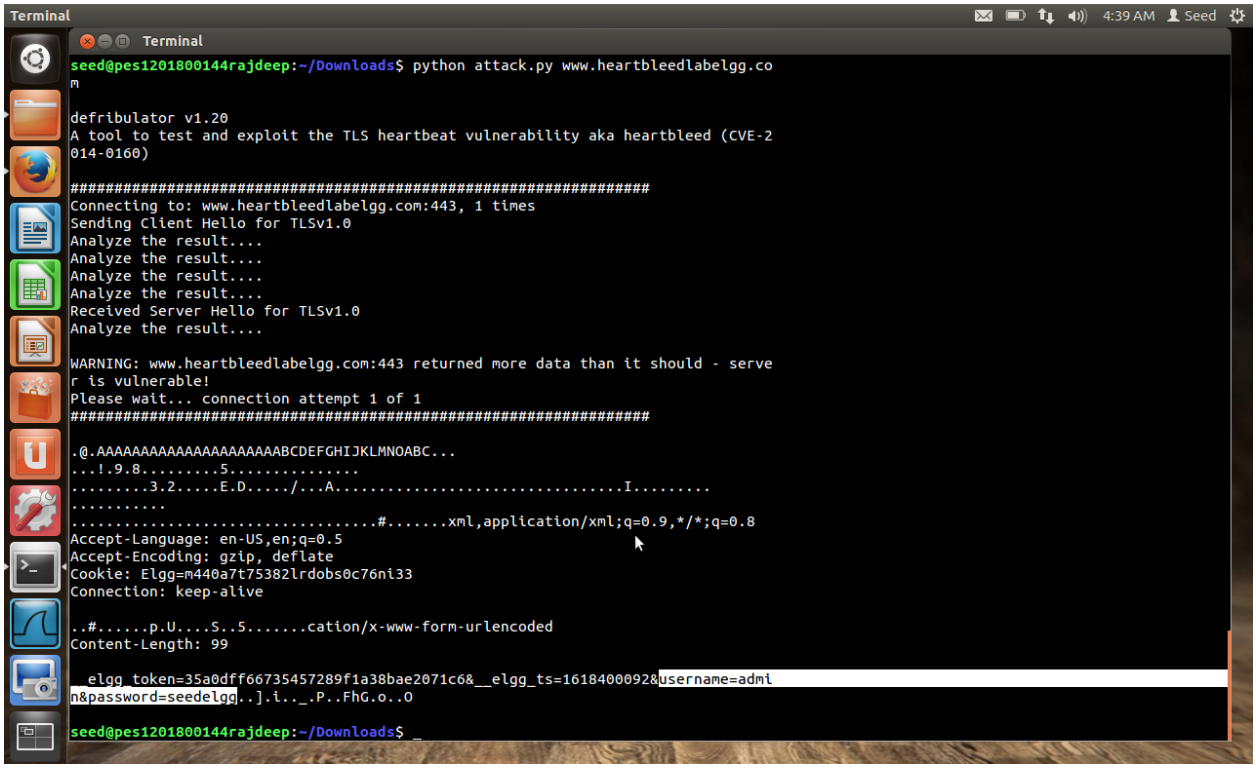
Screenshot 2: Running the attack

Random values are read from the server's memory which can be valuable once some action(login, sending message) happens on the server. In the above screenshot, we can see some random values in the server's memory but as we proceed with the below tasks, we will be able to find useful data in the server's memory.

TASK 2(a): USERNAME AND PASSWORD



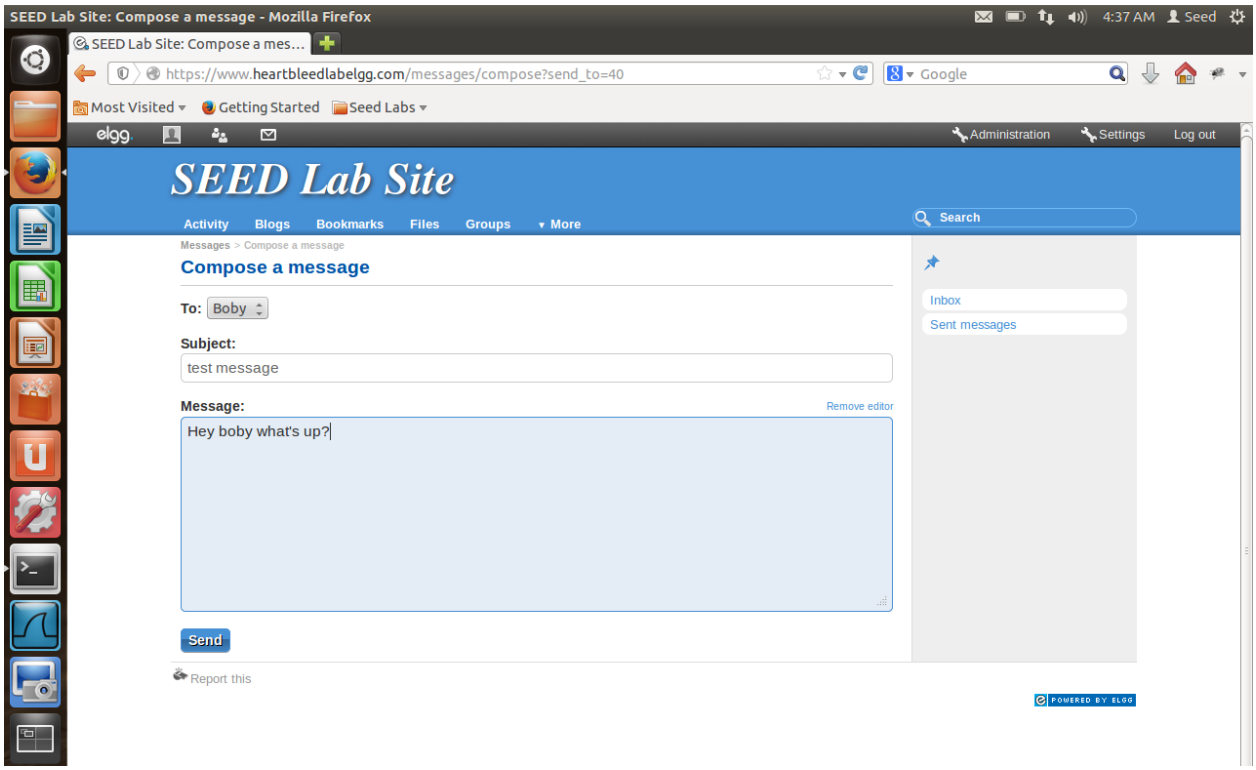
Screenshot 2a.1: Adding Boby as friend in admin profile



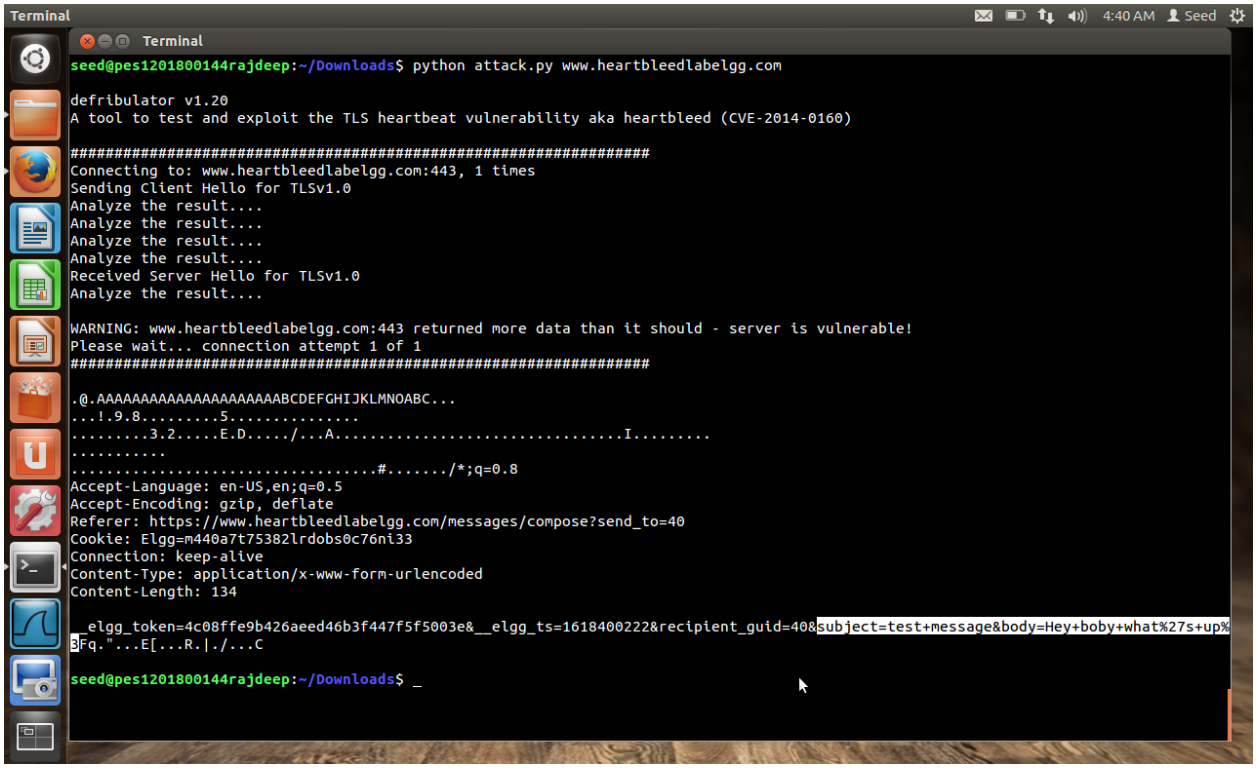
Screenshot 2a.2: Getting Username and Password in Heartbleed Attack

Executing the attack.py file repeatedly, we can capture the username and password of the admin who logs in which can be seen in the above screenshot.

TASK 2(b): SENDING PRIVATE MESSAGE



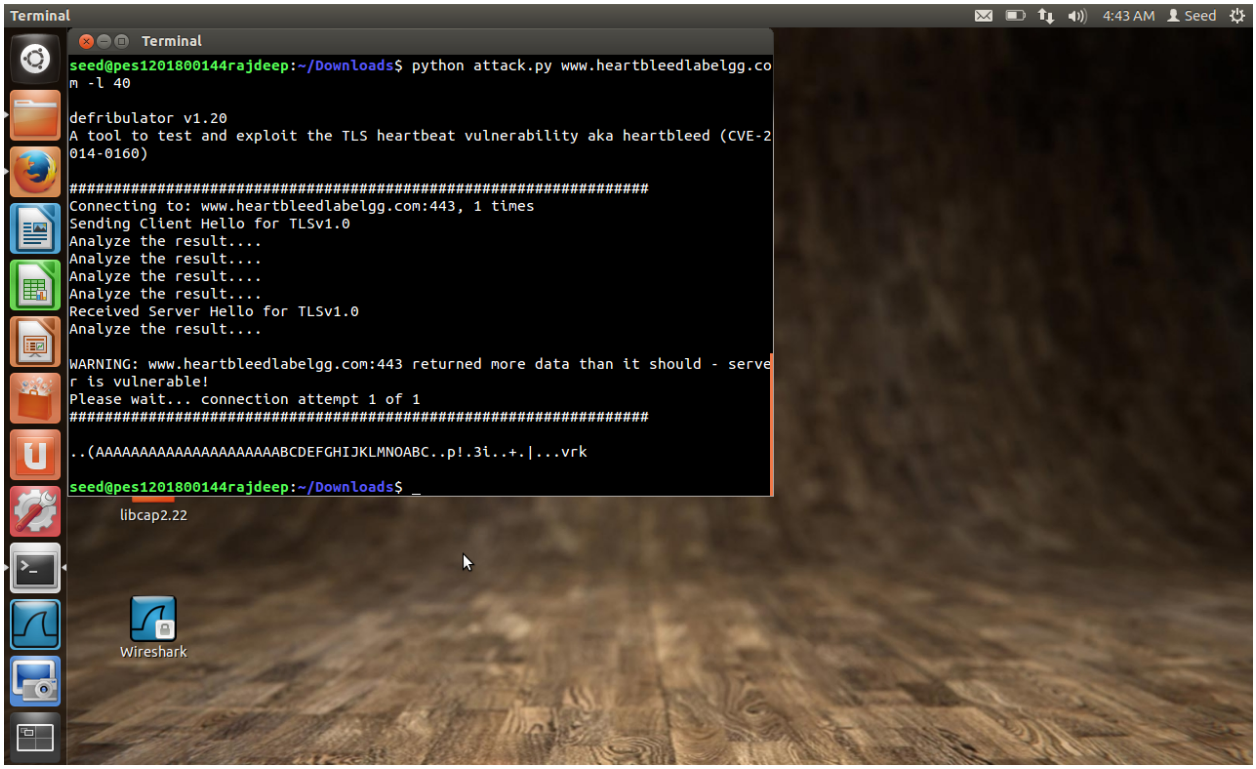
Screenshot 2b.1: Sending private message from admin profile to Boby



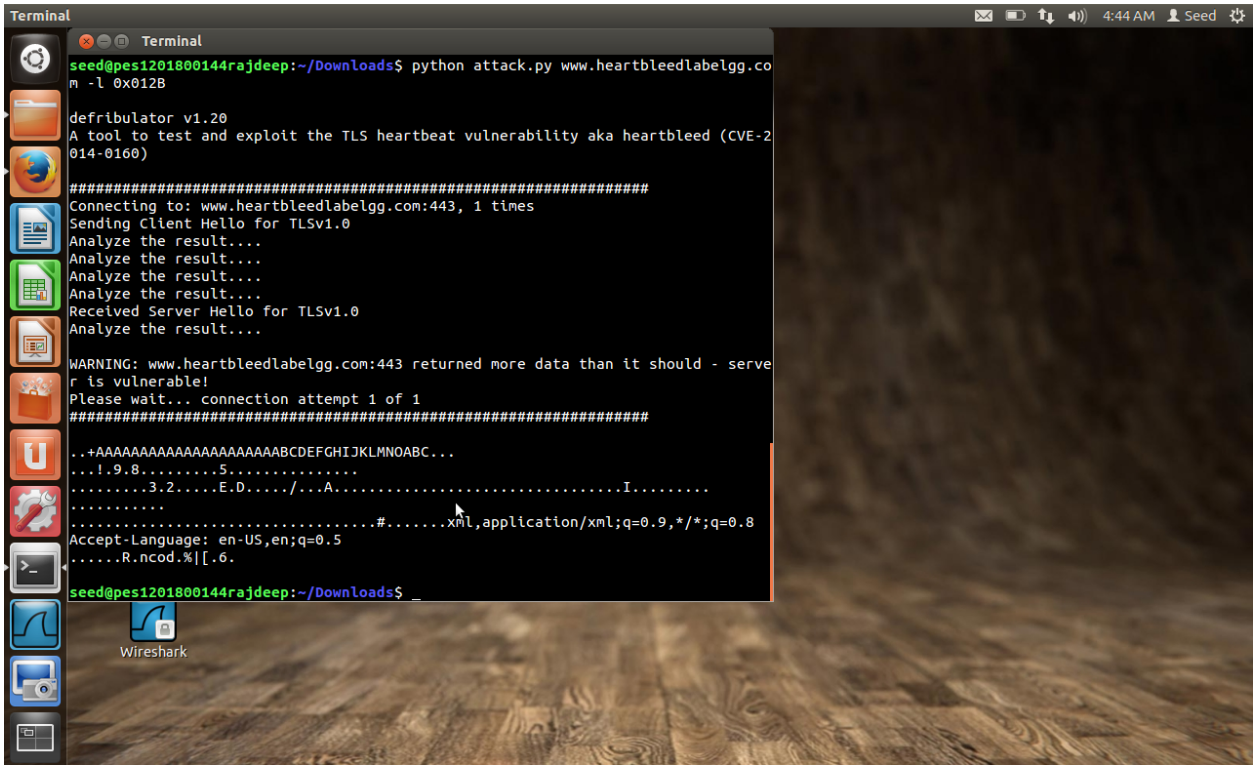
Screenshot 2b.2: Getting message in heartbleed attack

Executing the attack.py file repeatedly, we can capture the private message sent from admin to Boby as seen in above screenshot.

TASK 3: FUNDAMENTAL CAUSE OF HEARTBLEED ATTACK



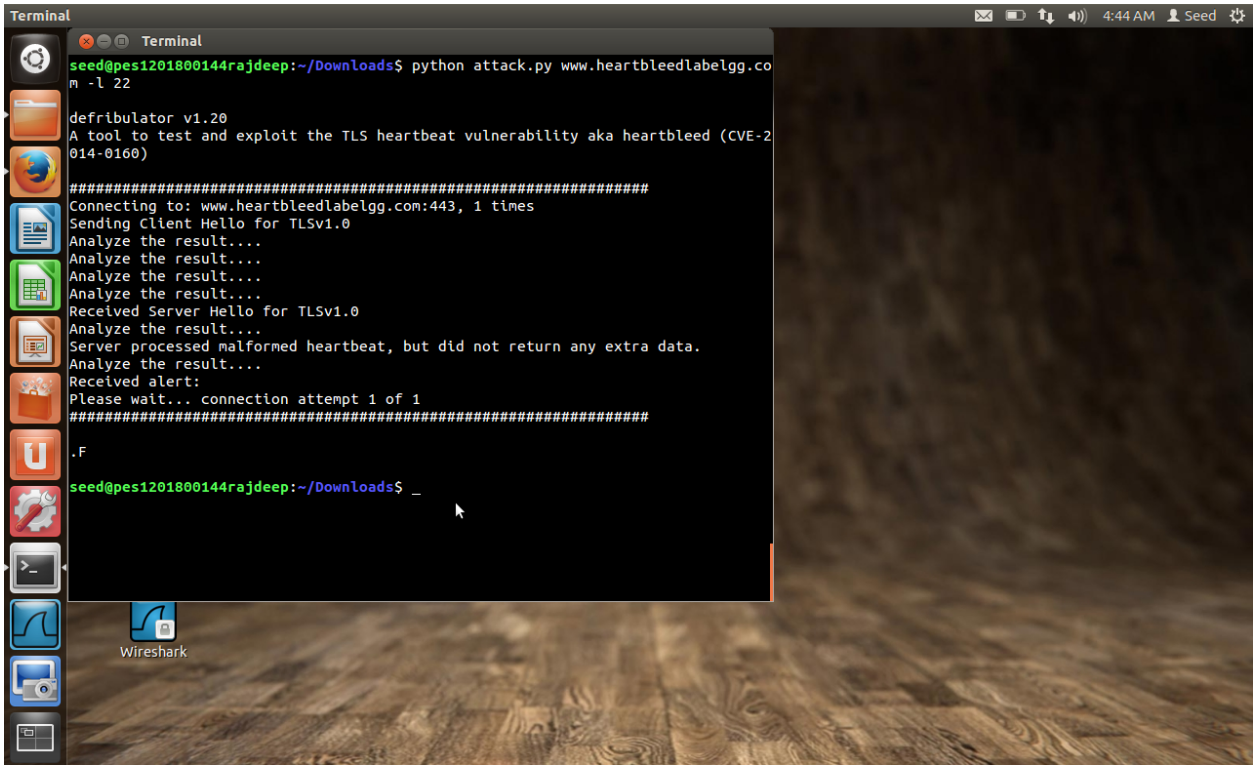
Screenshot 3.1: Payload length 40



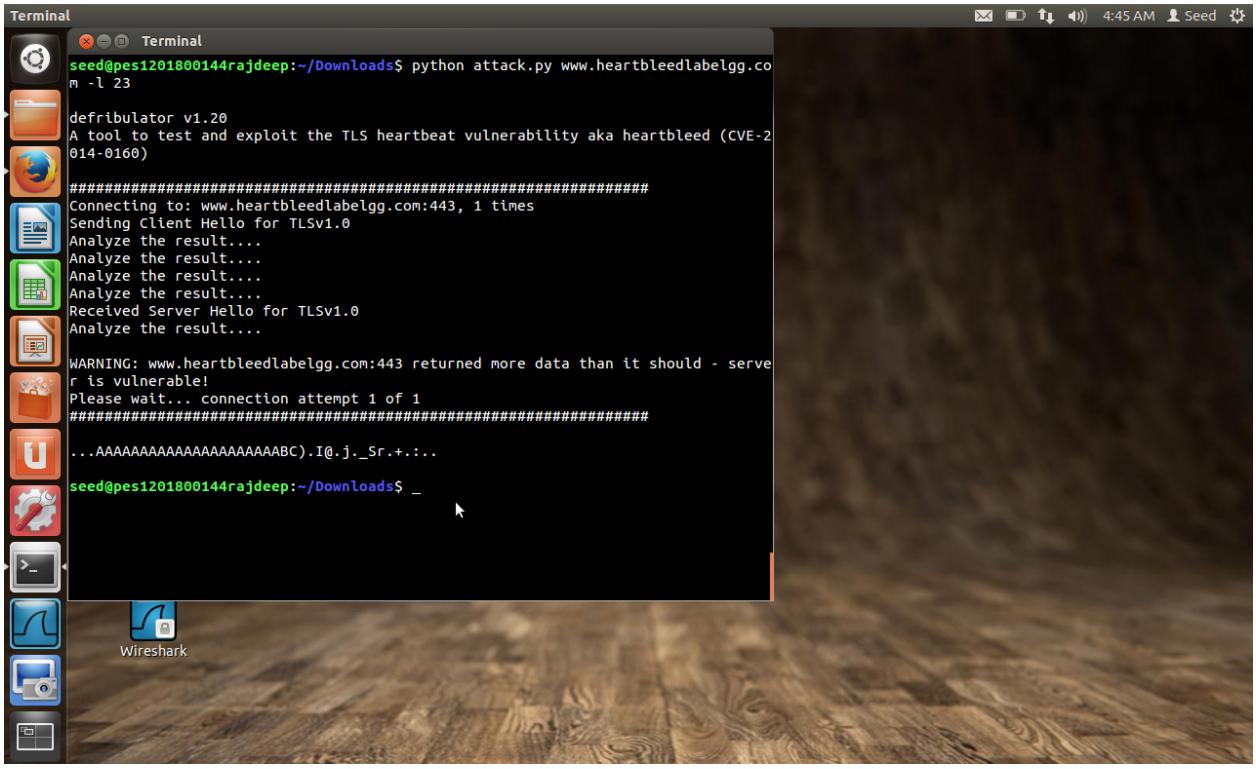
Screenshot 3.2: Payload length 0x012B

As the payload length value decreases, the length of data received from the server's memory decreases. But there is a boundary value till which the received data is the payload content and not the memory values of server.

TASK 4: FINDING THE BOUNDARY VALUE OF PAYLOAD LENGTH



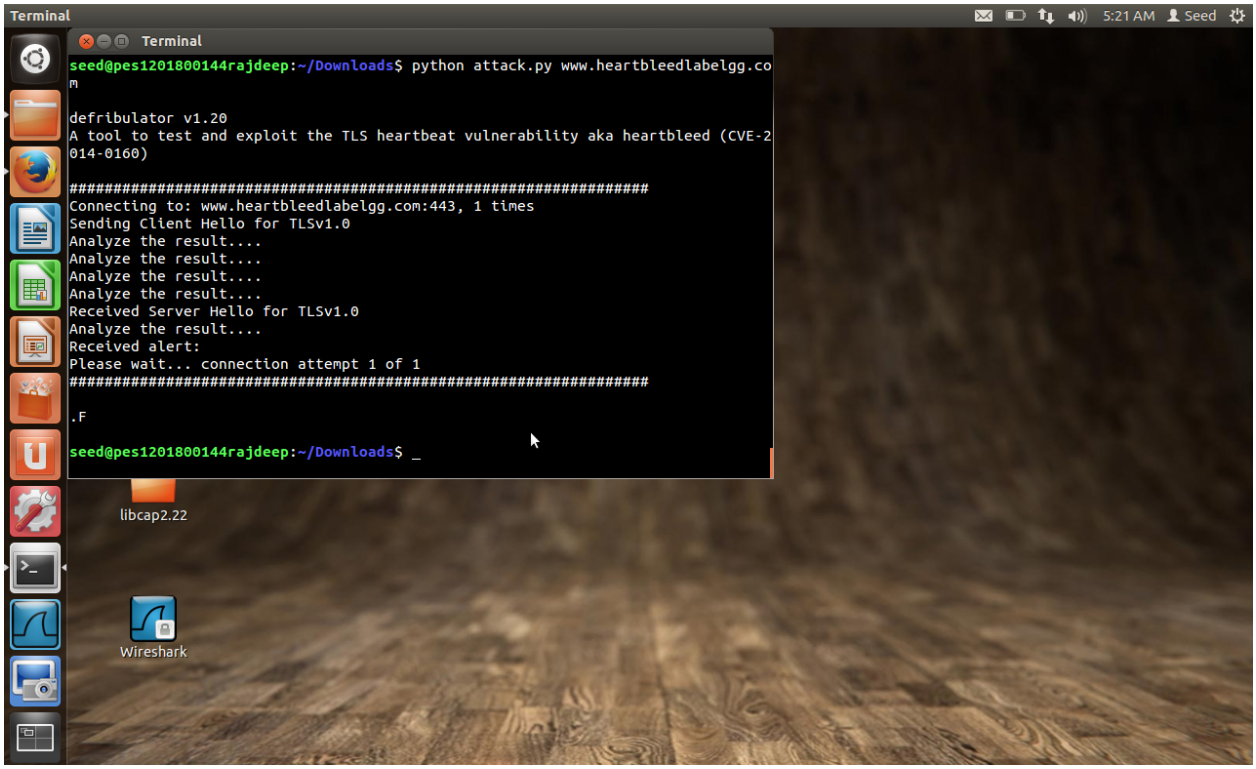
Screenshot 4.1: Payload length 22 reading properly



Screenshot 4.2: Payload length 23 reading extra memory

We can find in the above screenshot that when the payload length is 23 then the memory read is happening through the heartbleed bug. Whereas when the length is 22 then the payload content is read properly without memory read. Hence the boundary of payload length is 22.

TASK 5: COUNTERMEASURE



Screenshot 5.1: Heartbleed attack not able to read extra memory

Updating and upgrading the OpenSSL library,

```
$ sudo apt update
$ sudo apt upgrade
```

The heartbleed vulnerability is patched. This is done through the matching the actual payload size and the payload length given.
This is done through the following code:

```
hbtype = *p++;
    n2s(p, payload);
    if(1+2+payload+16 > s->s3->rrec.length)
        return 0; /* discard packet */
    p1 = p;
```

In this code, the actual packet size is matched with the length of (header type + payload length + payload content + padding).

1 bit → heartbeat packet type(request) field
2 bits → payload length field
payload → length of payload content
16 bits → padding field
s->s3->rrec.length → length of actual packet

==========

QUESTIONS ASKED:

Task 1: Find out username and password

Refer to Screenshot 2a.2

Task 2: Find out exact content of the private message.

Refer to Screenshot 2b.2

Task 3: Investigating the fundamental cause by using length = 40

Refer to Screenshot 3.1 and 3.2

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

Refer to Screenshot 4.1. The boundary value is 22.

==========