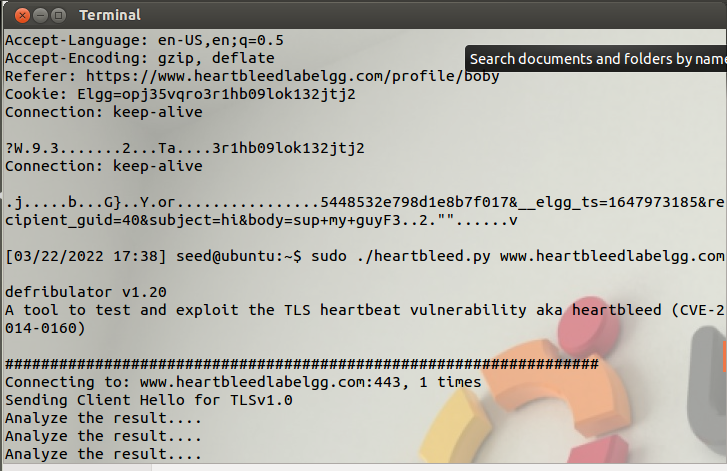
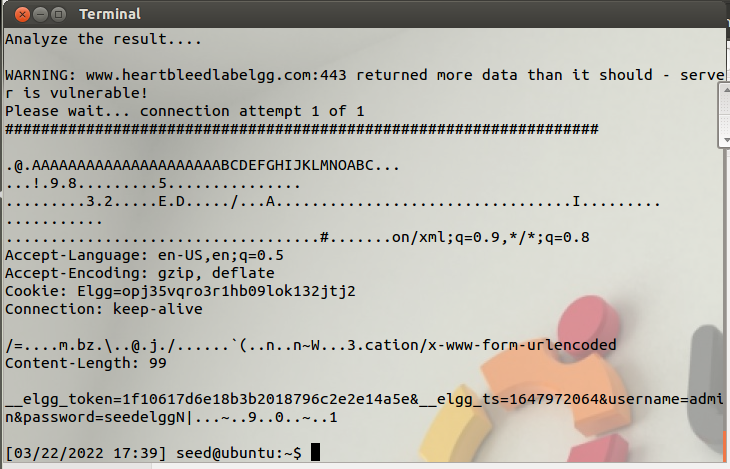
3.1 Response:

After sending multiple messages on the victim machine to users we were able to get the Admin username and password and get the subject and body of a message:

3.2: Vulnerability Cause:

Question 2.1: As the length variable decreases, the likelihood we extract any meaningful data goes down. The data itself was sometimes messed up as well (i.e. the message subject line wasn’t the whole thing).

Question 2.2: The highest length parameter that would return “Server processed malformed Heartbeat, but did not return any extra data” was a length of 22.

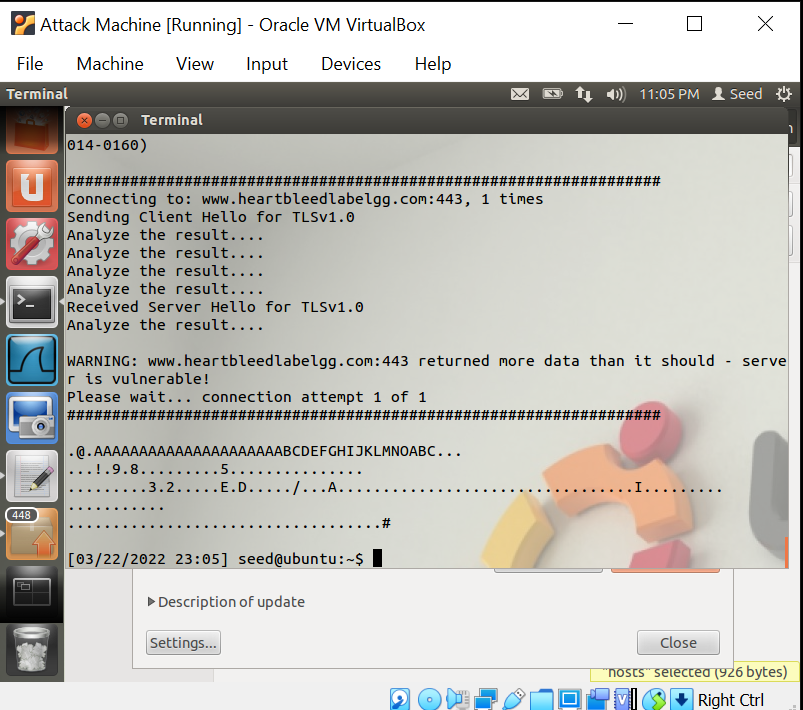
3.3: Vulnerability Patched:

Task 3.1:

After performing the command,

**sudo sed -i -e 's/archive.ubuntu.com\|security.ubuntu.com/old-releases.ubuntu.com/g' /etc/apt/sources.list**

,To update our repo source list on the victim server, the attacker is unable to retrieve anything from the victime server and i will only have the output below:



Task 3.2:

The problem in the code snippet is that there is nothing to check the lengths before they are used. There needs to be 2 checks implemented, one that checks if the heartbeat packet has a length greater than 0. And another check to see if the payload is the same length as the one provided by the user giving the input. If any of these checks fails then we make our program terminate. These checks would need to be implemented before the code snippet containing:

hbtype = \*p++;

n2s(p, payload);

pl=p;

Alice thinks the fundamental cause is missing the boundary checking during the buffer copy - this is incorrect, because even if there was a check for when the buffer boundary was reached, the calculated boundary would still be incorrect because the user-entered payload length is used in calculating it.

Bob thinks the cause is missing the user input validation - this is the correct fix, because the actual patch makes sure that the payload length, a user input variable, is actually correct.

Eva thinks that we can just delete the length value from the packet to solve everything - this would cause more harm than it would fix, because you would no longer know when the payload ends.