Information Security HandsOn Approach HW7

60947045s 呂昀修

Jan, 24, 2022

1. **HeartBleed Attack SEED Lab**

   Task1.
   When I run attack.py first time, I get the useful information: password; then I go 8 times and get the private message; finally, it runs same result again for each 10 times.

Figure 1

Figure 2

Task2.

Figure 3: I add the payload length with 2000 and find that it returns more characters (red line)

Then I decrease the length number, it returns less extra contents:

Figure 4

Figure 5

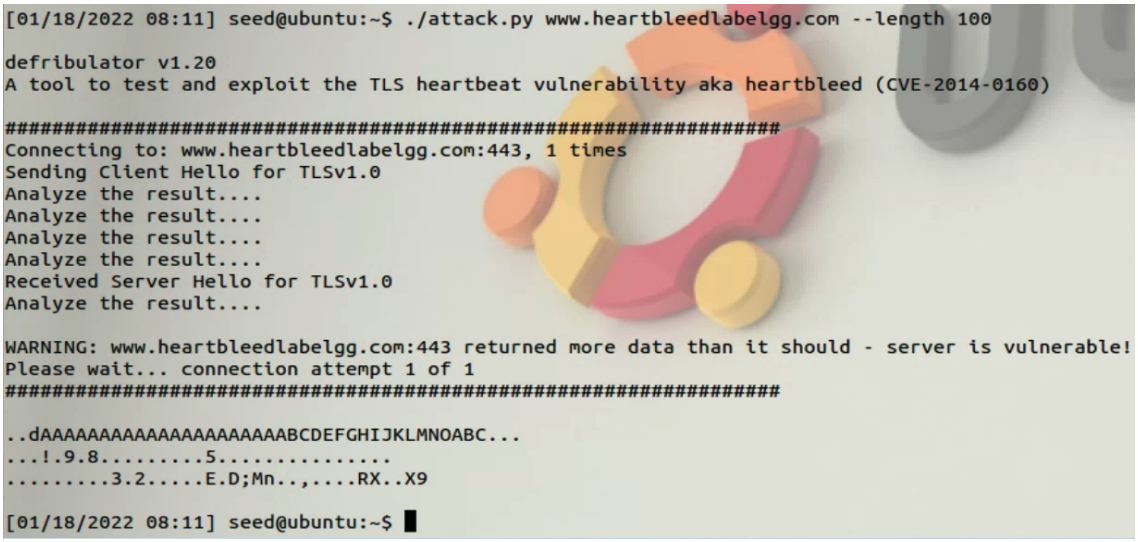

Figure 6

When the length number equals 22, it returns ""Server processed malformed Heartbeat, but did not return any extra data.":

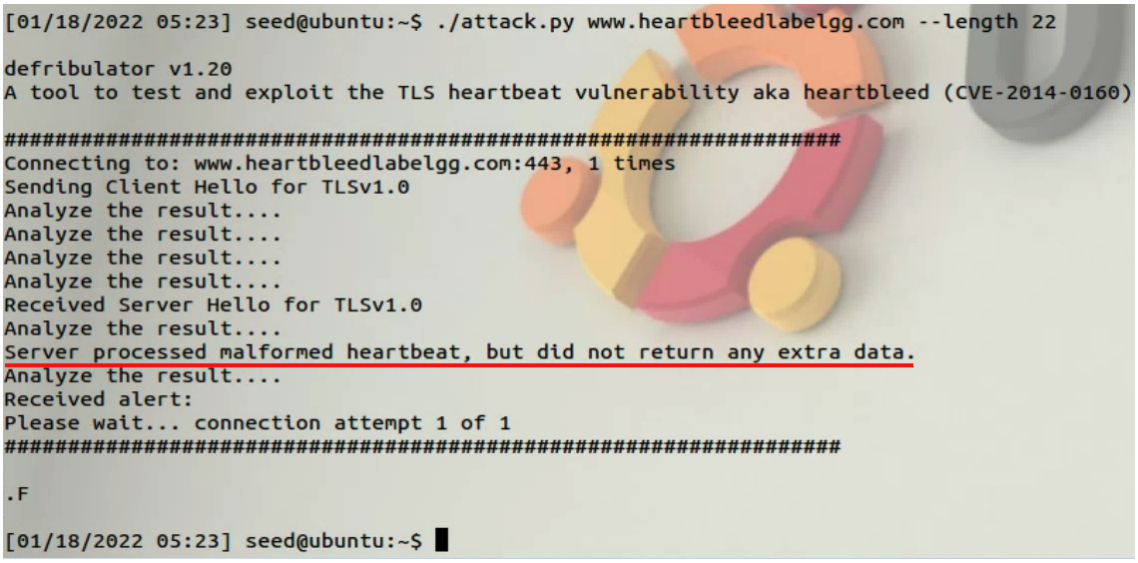

Figure 7

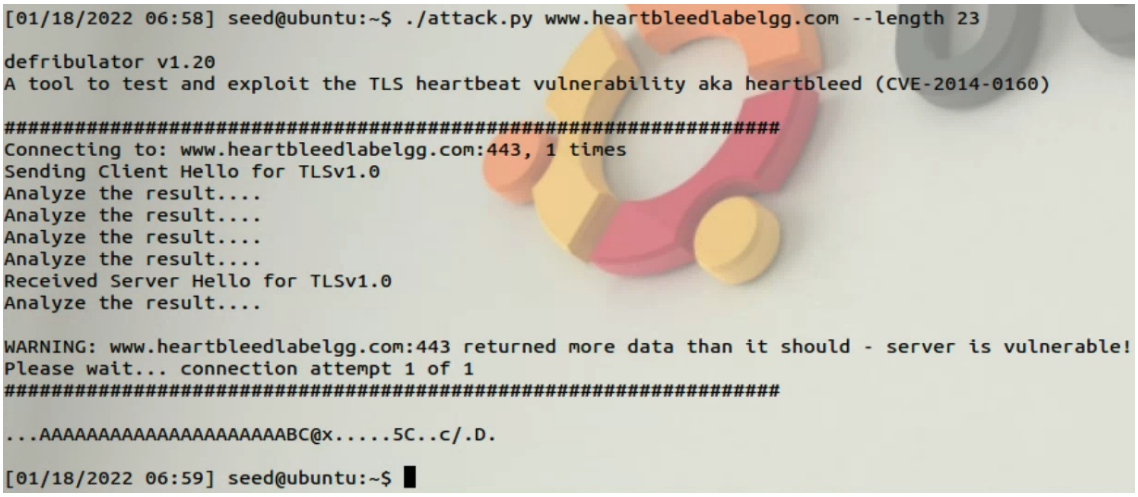

Figure 8: length number 23 still returns extra contents

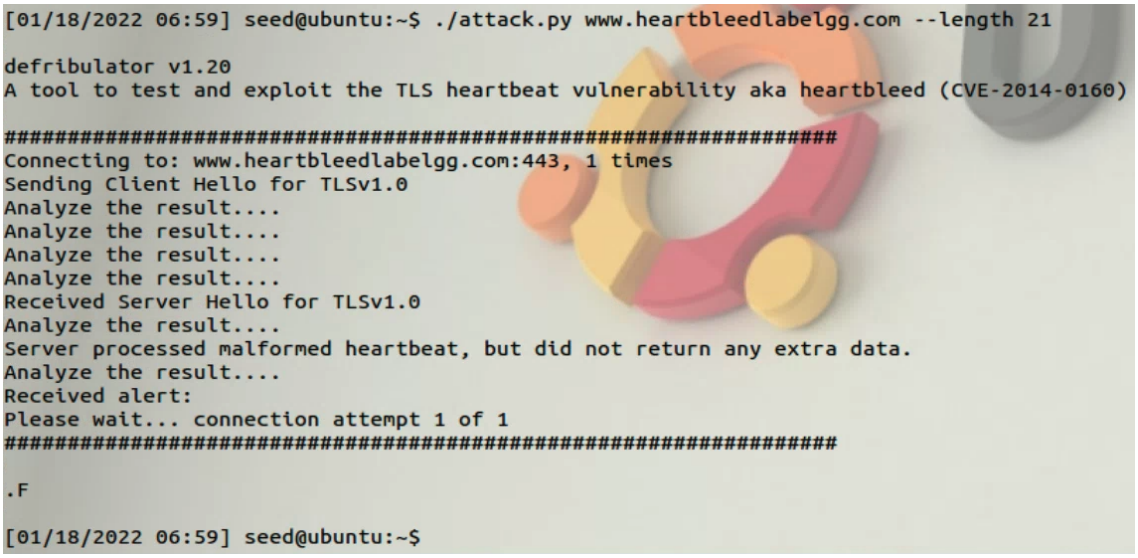

Figure 9: below 22, it didn't return any extra data

Task3.
Here comes a problem when updating apt-get: ubuntu12 is too old to do apt-get update and apt-get upgrade, so the solution is updating ubuntu12 to ubuntu14. After that, execute the attack.py again, it shows that the attack is failed.

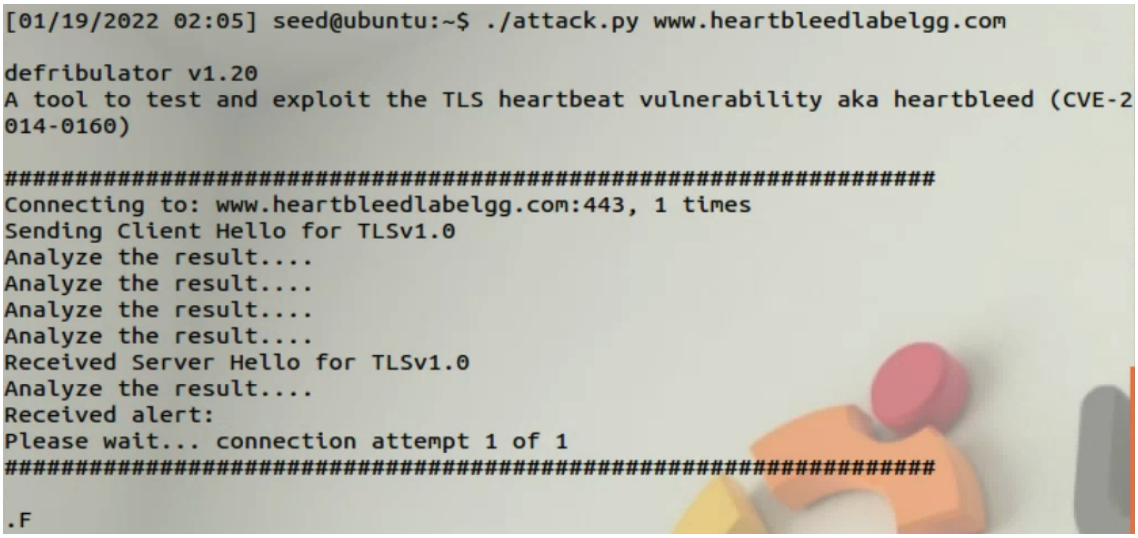

Figure 10

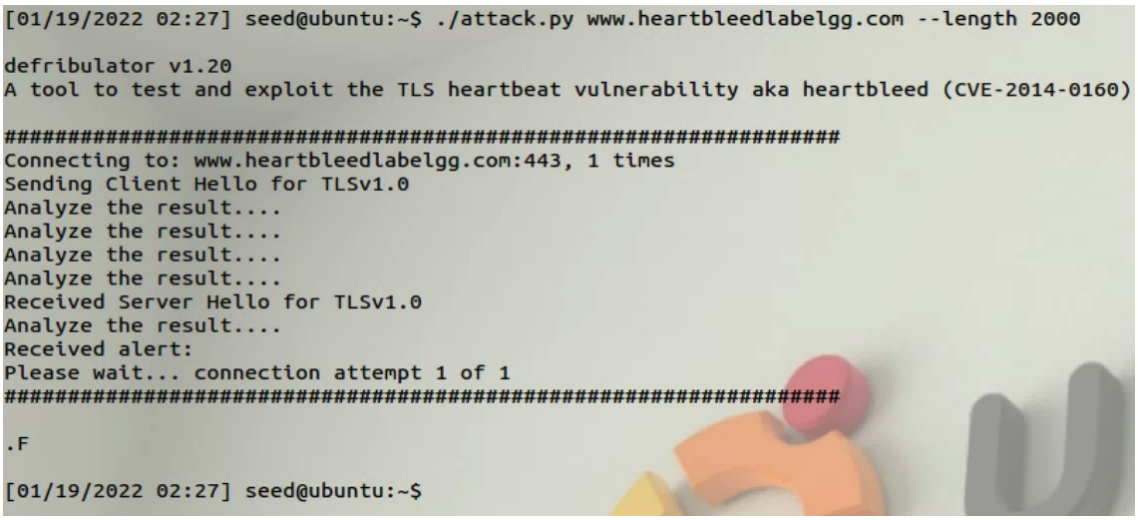

Figure 11

How to fix the bug is to check whether the decipher payload length is larger than the receiving payload length; if so, discard the request packet and don't response. (Add the condition right after 'n2s(p, payload)')
Comment:
Alice thinks the fundamental cause is missing the boundary checking during the buffer copy: It is similar to the original solution, check the boundary if there are illegal contents.
Bob thinks the cause is missing the user input validation: I think it's not a good solution because if we check user input of each packet, that would be very inefficient.
Eva thinks that we can just delete the length value from the packet to solve everything: