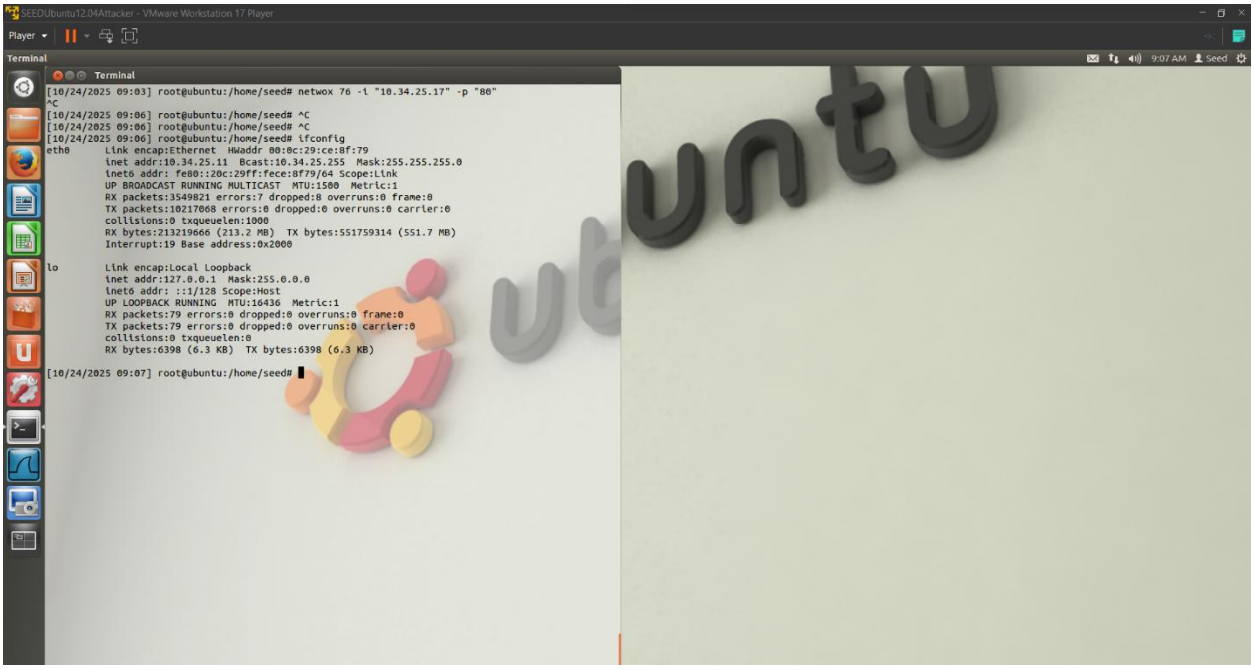
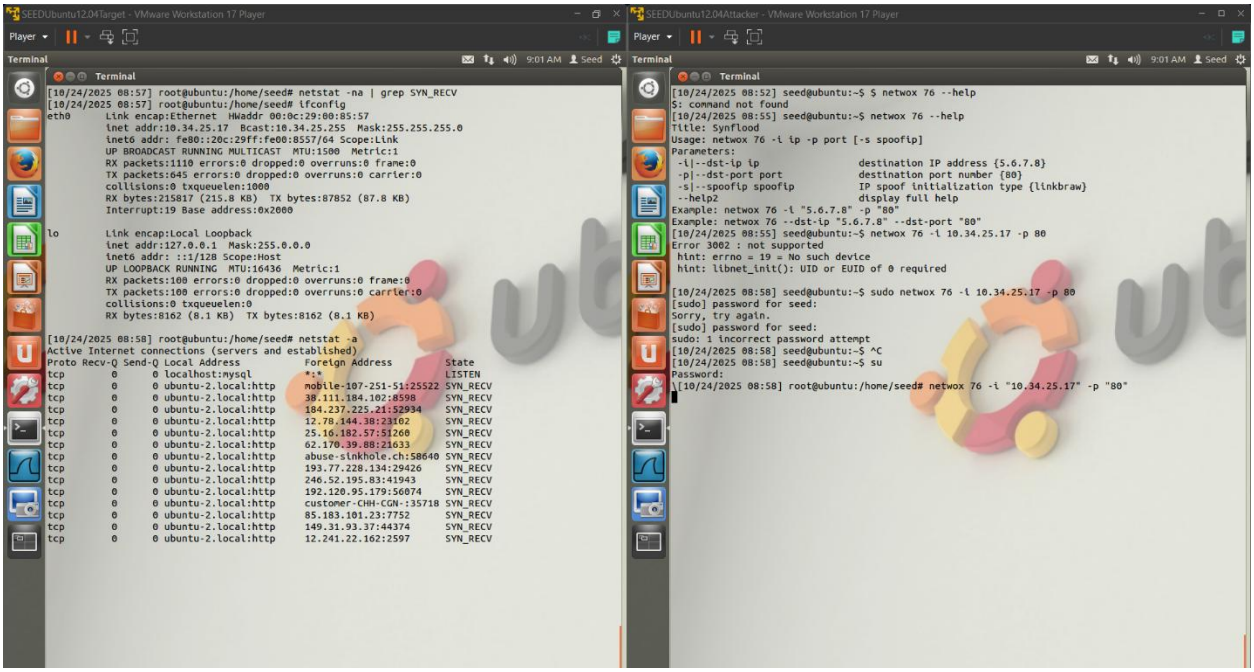
Q1. What is the attacker's IP address?

ANS 10.34.25.11



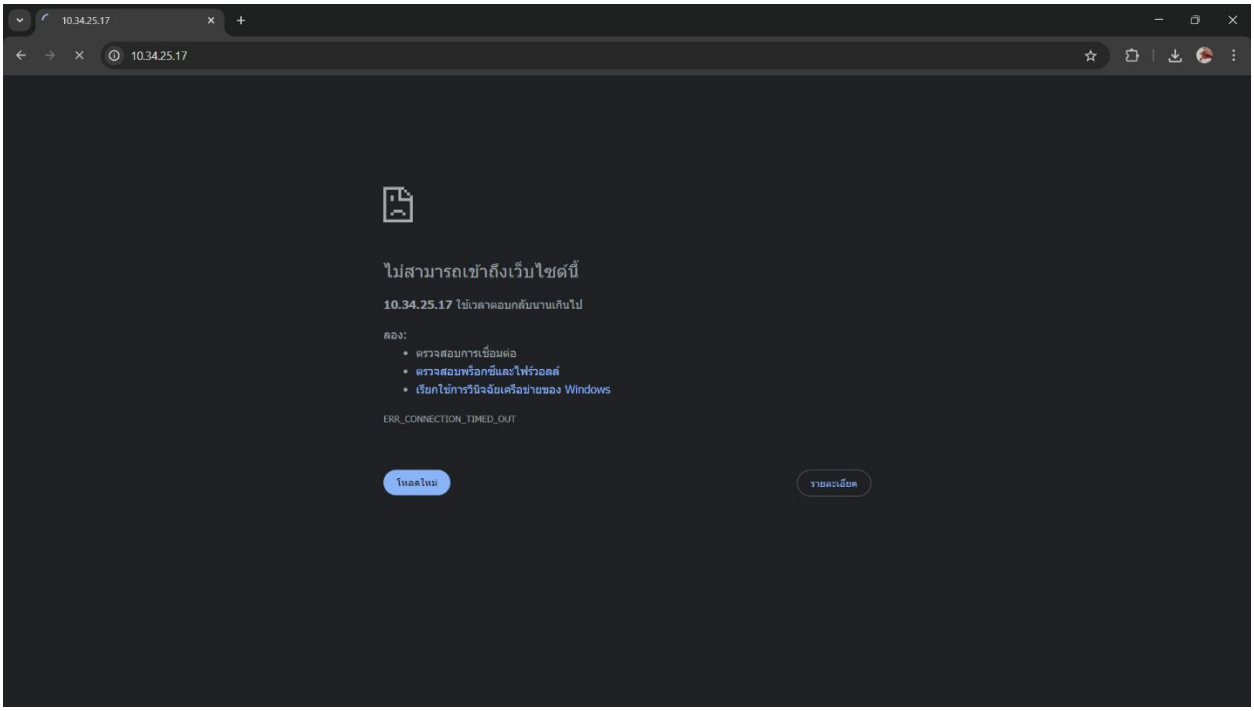
Q2. What command did you use to run the attack?

ANS netwox 76 -i “10.34.25.17” ip “80”



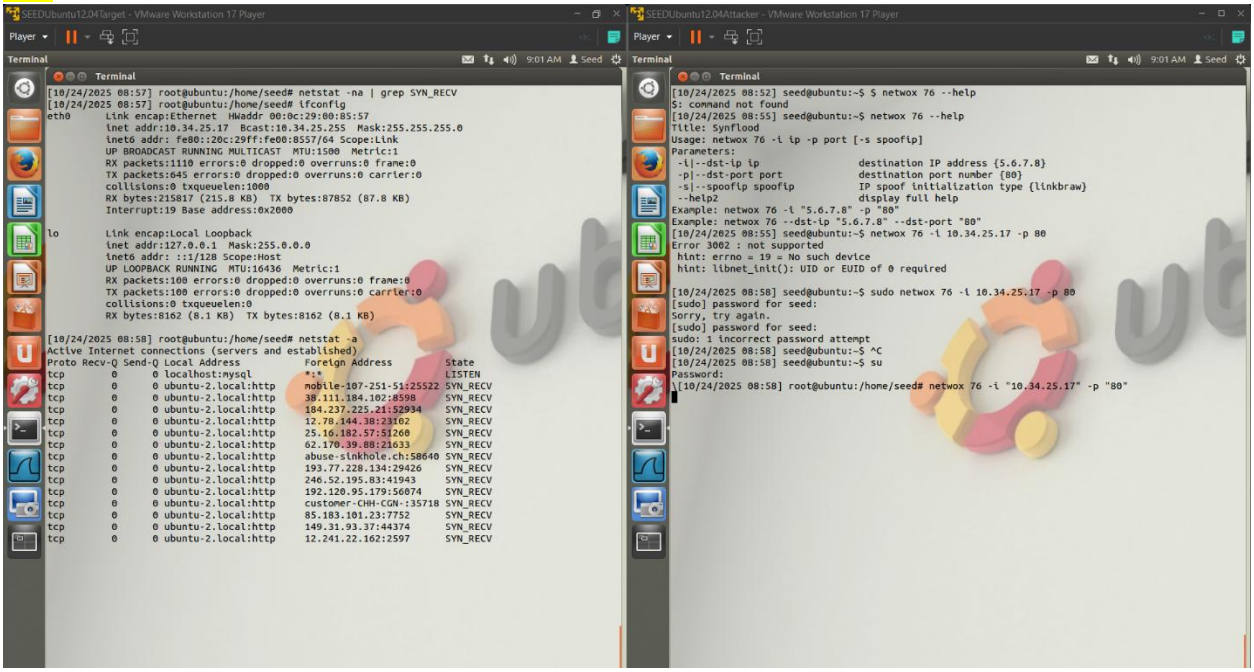
Q3. How do you know the attack is successful? Hint: Use the browser on your notebook to access the webpage. What should happen if the attack is successful?

ANS can’t access the target



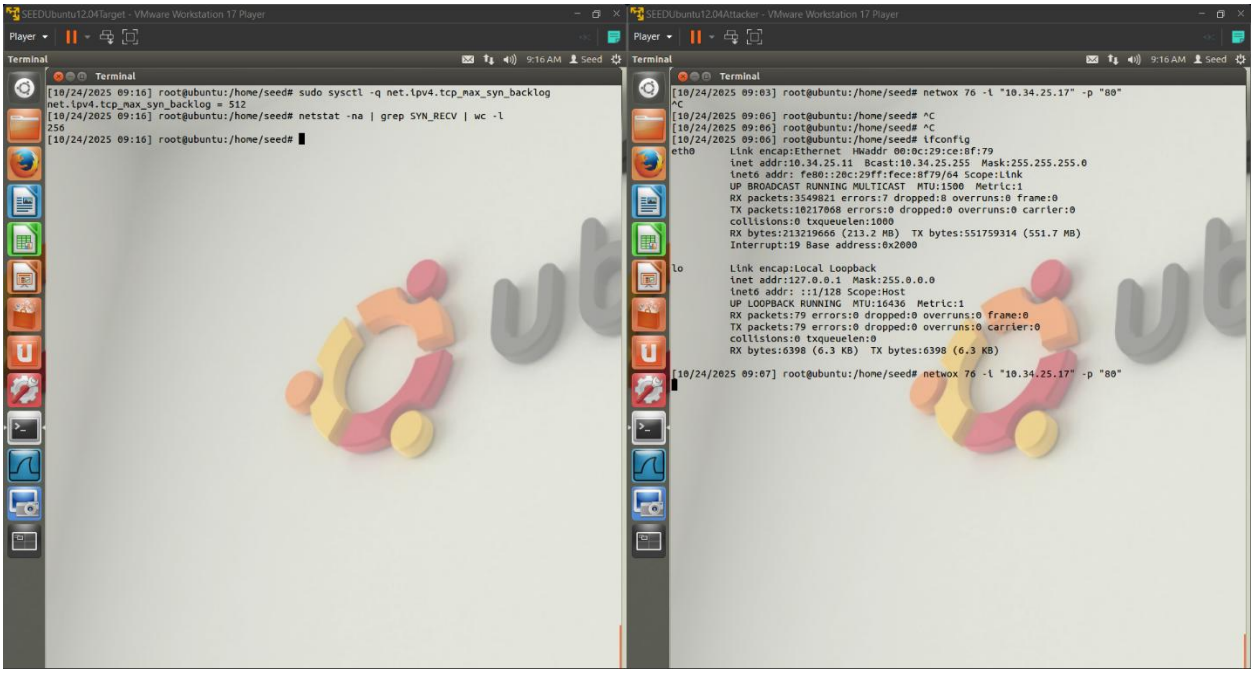
Q4. “netwox” performs the TCP SYN Flood attack using spoofed IP addresses. Give some examples of the spoofed IP addresses you see on the target machine.

ANS 38.111.184.102, 184.237.225.21, …



Q5. In the TCP SYN Flood attack, what resource on the server side is exhausted? What is the number of resources available, and how many of those resources get used up in the attack?

ANS SYN backlog / queue for half-open connections, 512, 256

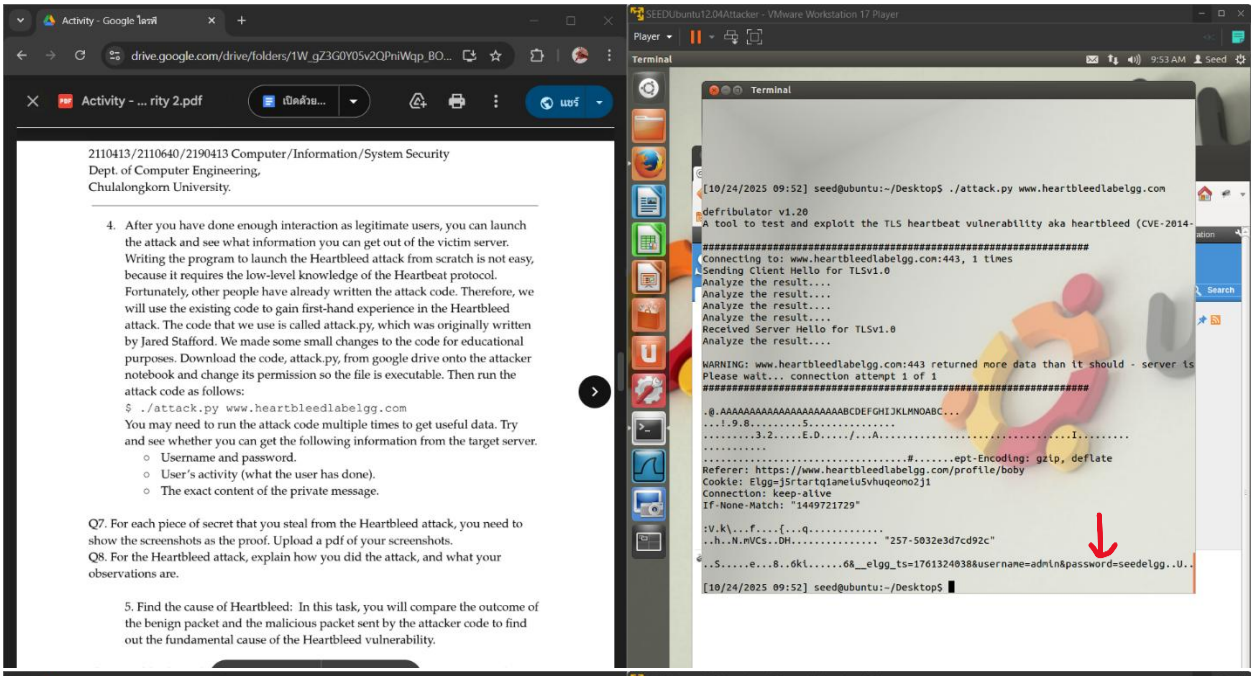


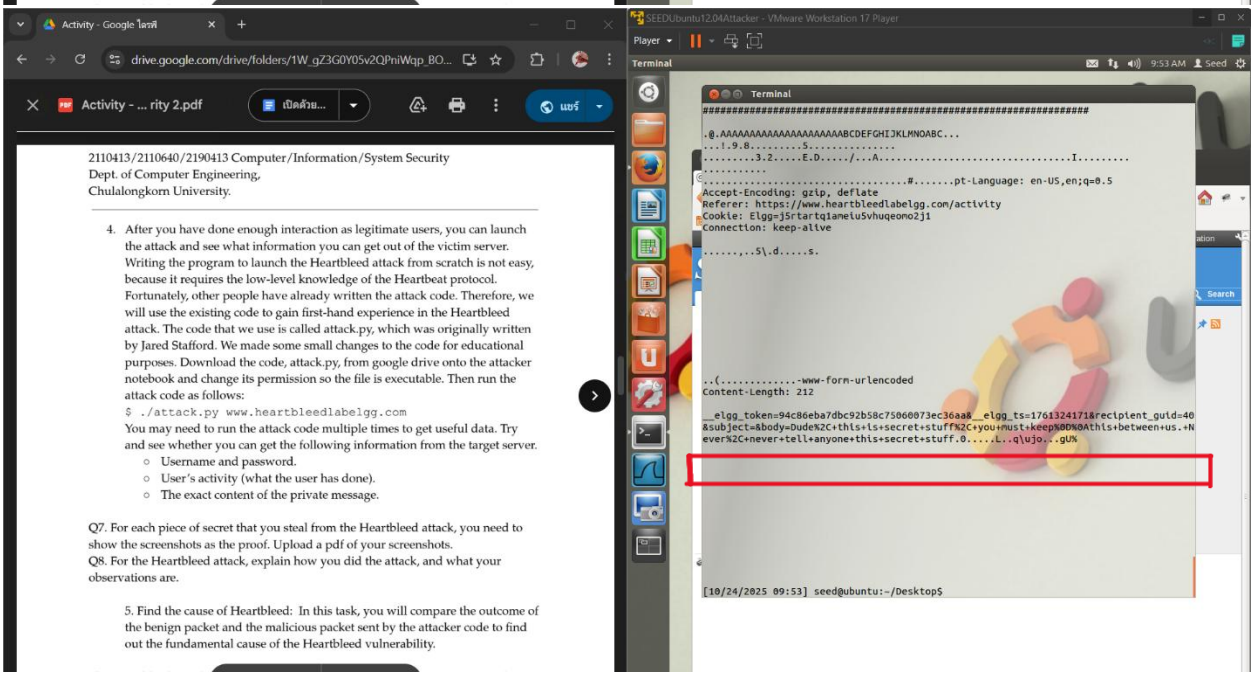
Q6. How do TCP SYN cookies prevent this type of attack?

ANS SYN cookie ทำงานโดย **ไม่จองหน่วยความจำสำหรับการเชื่อมต่อที่ยังไม่สมบูรณ์** เมื่อเซิร์ฟเวอร์ได้รับ SYN ปกติ มันจะเก็บ entry ใน backlog และส่ง SYN-ACK กลับ แต่เมื่อเปิด SYN cookie เซิร์ฟเวอร์จะไม่สร้าง entry ในนั้น ถ้าเซิร์ฟเวอร์ไม่ต้องจองหน่วยความจำล่วงหน้า ⟶ backlog ไม่ถูกเติมเต็มจาก half-open connections ปลอม ⟶ เซิร์ฟเวอร์ยังคงรับการเชื่อมต่อที่ถูกต้องได้

Q7. For each piece of secret that you steal from the Heartbleed attack, you need to show the screenshots as the proof. Upload a pdf of your screenshots.

ANS





Q8. For the Heartbleed attack, explain how you did the attack, and what your

observations are.

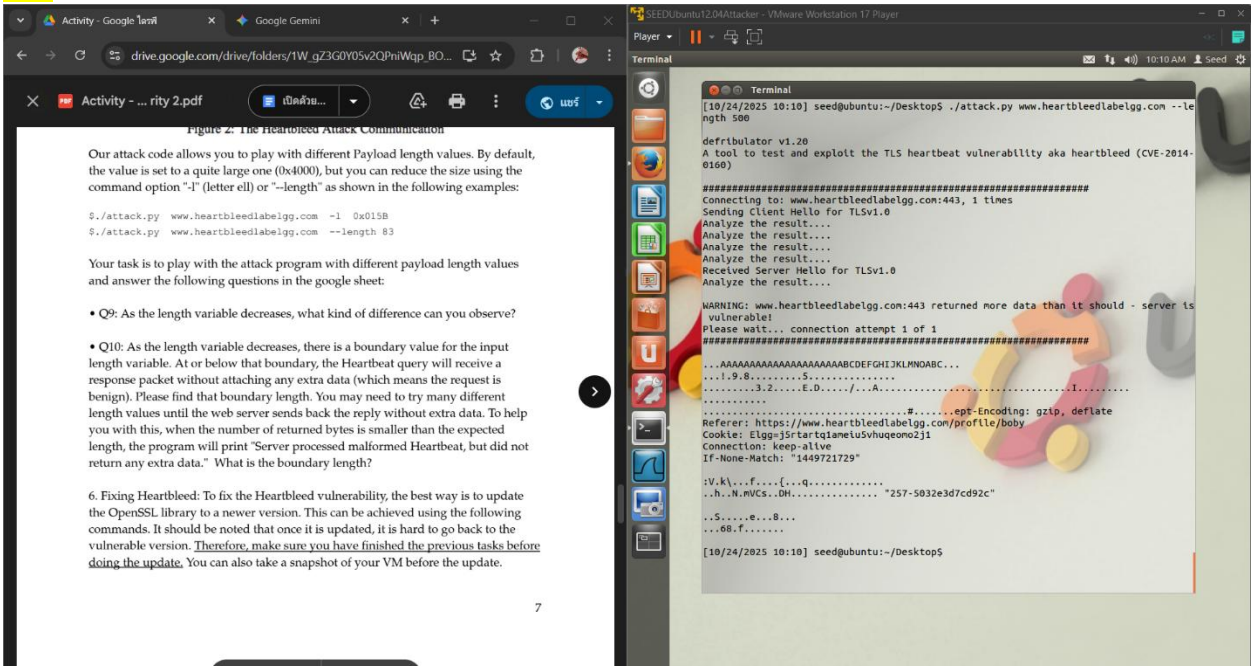
ANS

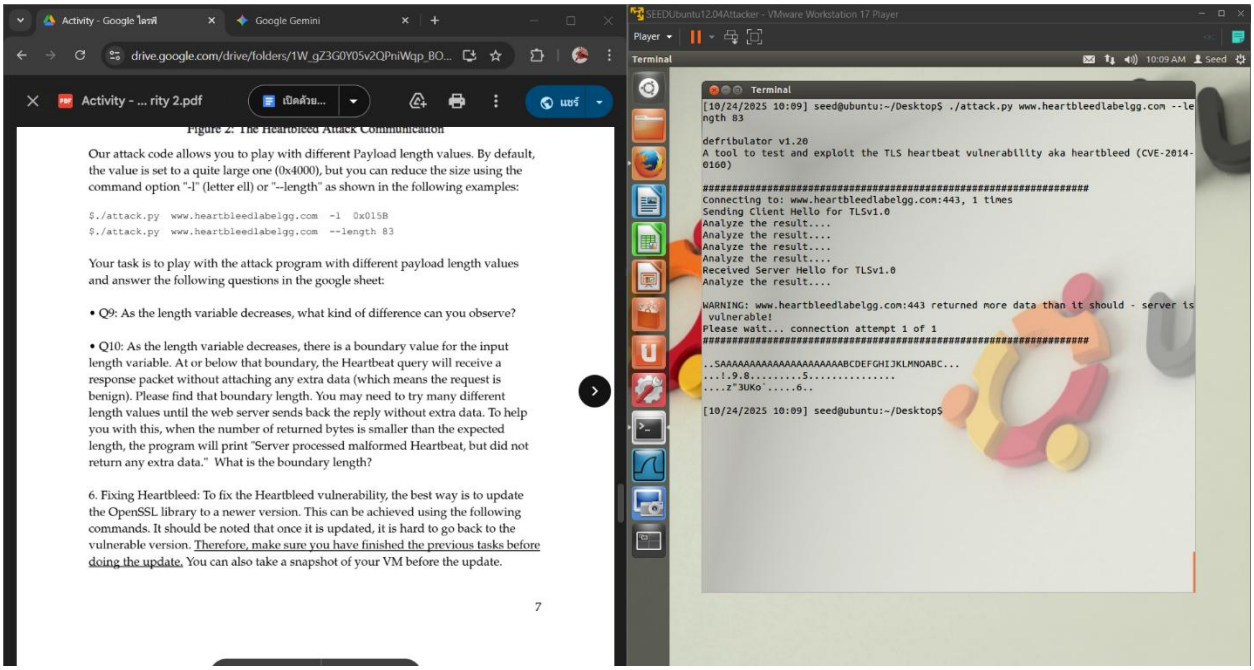
Preparation: Before the attack, an attacker logged into the web app and performed sensitive actions("Dude, this is secret stuff...") to ensure secret data was present in the server's memory .

Execute: used the provided Python exploit code, **attack.py**, against the target domain.

Q9: As the length variable decreases, what kind of difference can you observe?

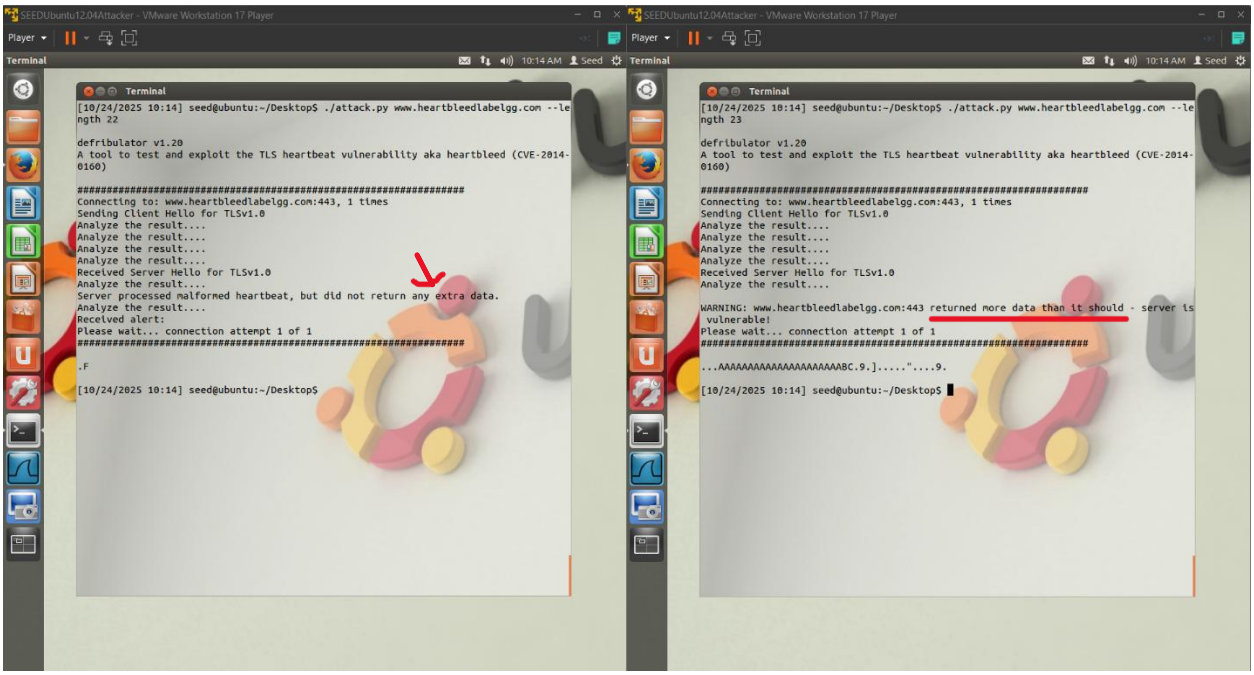
ANS small length -> small data from target memory



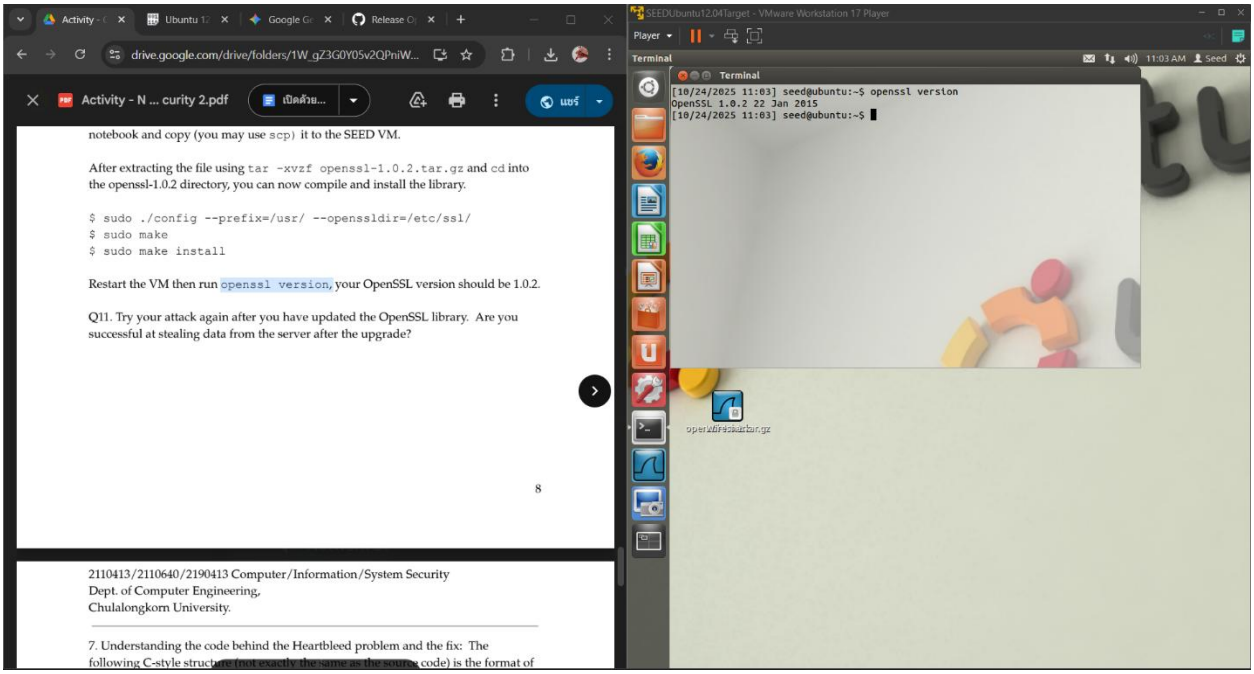


Q10: As the length variable decreases, there is a boundary value for the input length variable. At or below that boundary, the Heartbeat query will receive a response packet without attaching any extra data (which means the request is benign). Please find that boundary length. You may need to try many different length values until the web server sends back the reply without extra data. To help you with this, when the number of returned bytes is smaller than the expected length, the program will print "Server processed malformed Heartbeat, but did not return any extra data." What is the boundary length?

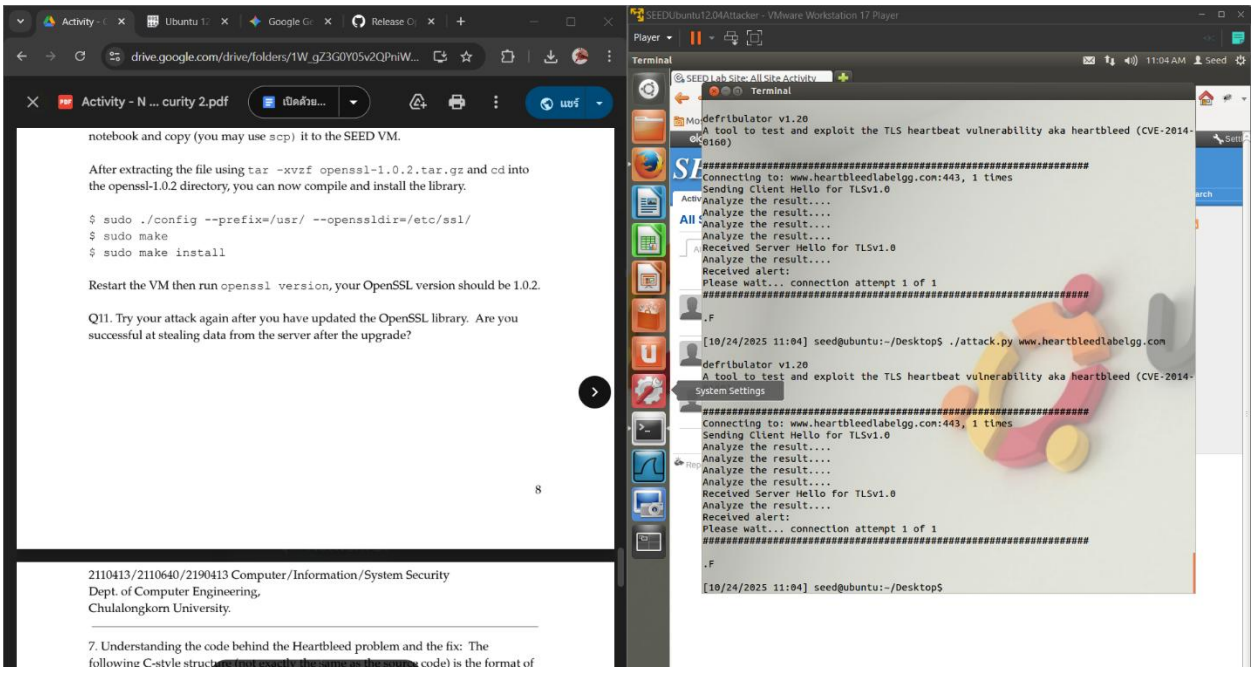
ANS 22



Q11. Try your attack again after you have updated the OpenSSL library. Are you successful at stealing data from the server after the upgrade?



ANS NO



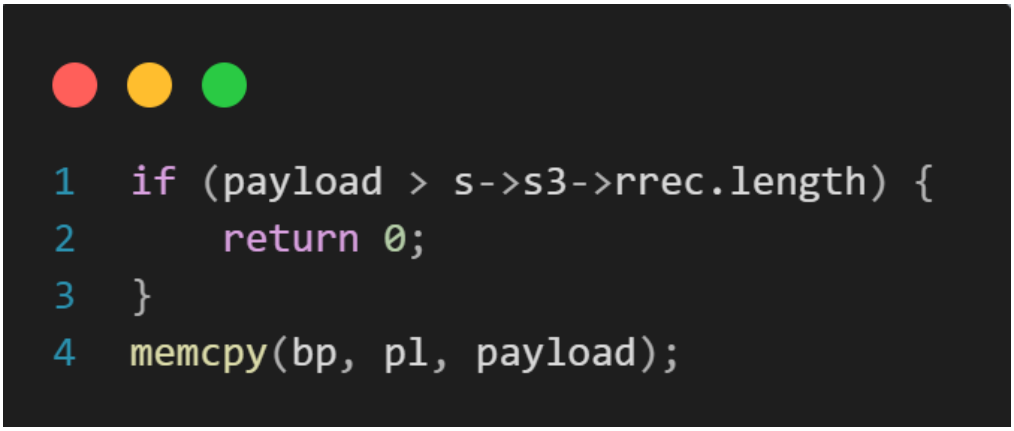
Q12. Please point out the problem from the code and provide a solution to fix the

bug (i.e., what modification is needed to fix the bug). You do not need to recompile

the code; just describe how you can fix the problem.

ANS The Heartbleed vulnerability is a **buffer over-read** caused by the server blindly trusting the payload length value from the request.

The fix involves introducing a **check (validation)** to ensure that the user-supplied payload length does not exceed the **actual size of the received Heartbeat message (line 40)**.



Q13. Comment on the following discussions by Alice, Bob, and Eva regarding the fundamental cause of the Heartbleed vulnerability: Alice thinks the fundamental cause is missing the boundary checking during the buffer copy; Bob thinks the cause is missing the user input validation; Eva thinks that we can just delete the length value from the packet to solve everything. Who do you agree and disagree with, and why?

ANS I agree with **Alice and Bob** because the problem is the **buffer over-read**, which **input validation** can fix. I disagree with **Eva** because without the payload length, the **server doesn't know** how much data to process.