Phatcharapon Jumruspun 6031040921

Q1

There are too many Ips as the attacker is spoofing his IP address, avoiding his identity.
But according to the netstat -na command, the real ip is 192.168.56.1

```
[09/28/2020 20:18] seed@ubuntu:~$ netstat -na | head -30
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 192.168.56.102:53       0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 192.168.56.102:80       192.168.56.1:50355      TIME_WAIT
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::3128                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
udp        0      0 192.168.56.102:53       0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:52430           0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:40399           0.0.0.0:*
udp6       0      0 :::53                   :::*
udp6       0      0 :::42126                :::*
udp6       0      0 :::5353                 :::*
udp6       0      0 :::42916                :::*
```

```
[09/28/2020 20:18] seed@ubuntu:~$ netstat -na | head -30
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 192.168.56.102:53       0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 192.168.56.102:80       192.168.56.1:50370      ESTABLISHED
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::3128                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
udp        0      0 192.168.56.102:53       0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 0.0.0.0:52430           0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:40399           0.0.0.0:*
udp6       0      0 :::53                   :::*
udp6       0      0 :::42126                :::*
udp6       0      0 :::5353                 :::*
udp6       0      0 :::42916                :::*
```

Picture showing the attacker's real IP

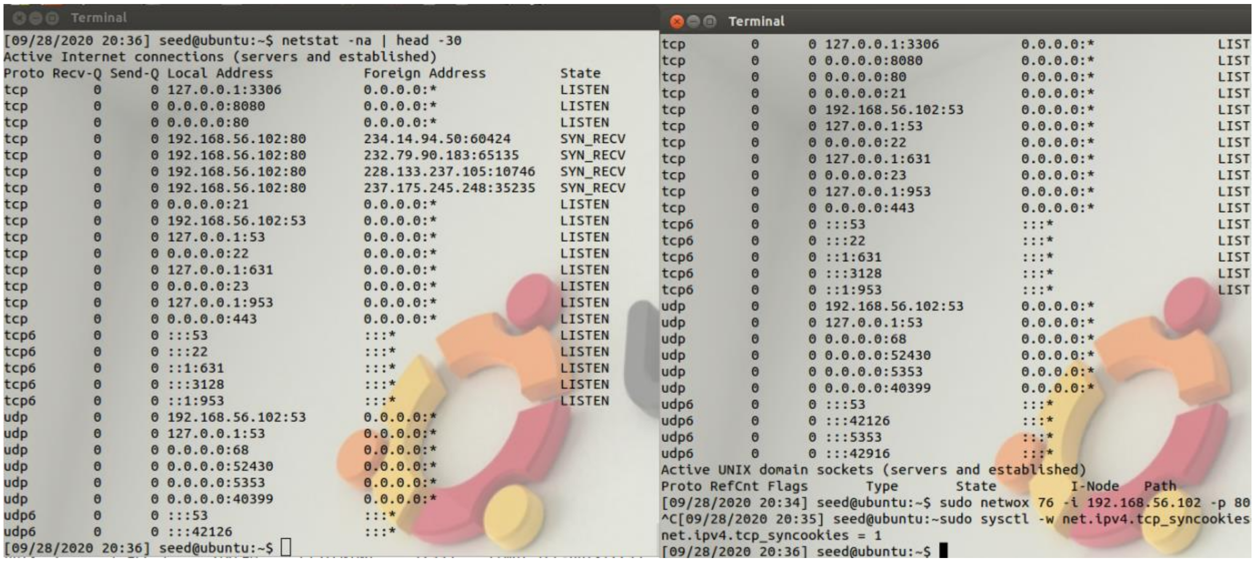
```
[09/28/2020 20:20] seed@ubuntu:~$ netstat -a | head -30
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:mysql         *:*                     LISTEN
tcp        0      0 *:http-alt              *:*                     LISTEN
tcp        0      0 *:http                  *:*                     LISTEN
tcp        0      0 *:ftp                   *:*                     LISTEN
tcp        0      0 ubuntu.local:domain     *:*                     LISTEN
tcp        0      0 localhost:domain        *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp        0      0 *:telnet                *:*                     LISTEN
tcp        0      0 localhost:953           *:*                     LISTEN
tcp        0      0 *:https                 *:*                     LISTEN
tcp        0      0 ubuntu.local:http       Phatcharapons-Mac:50370 TIME_WAIT
tcp6       0      0 [::]:domain             [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 localhost:ipp           [::]:*                  LISTEN
tcp6       0      0 [::]:3128               [::]:*                  LISTEN
tcp6       0      0 localhost:953           [::]:*                  LISTEN
udp        0      0 ubuntu.local:domain     *:*
udp        0      0 localhost:domain        *:*
udp        0      0 *:bootpc                *:*
udp        0      0 *:52430                 *:*
udp        0      0 *:mdns                  *:*
udp        0      0 *:40399                 *:*
udp6       0      0 [::]:domain             [::]:*
udp6       0      0 [::]:42126              [::]:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:42916              [::]:*
```

```
[09/28/2020 20:20] seed@ubuntu:~$ netstat -a | head -30
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 *:ftp                   *:*                     LISTEN
tcp        0      0 ubuntu.local:domain     *:*                     LISTEN
tcp        0      0 localhost:domain        *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp        0      0 *:telnet                *:*                     LISTEN
tcp        0      0 localhost:953           *:*                     LISTEN
tcp        0      0 *:https                 *:*                     LISTEN
tcp        0      0 ubuntu.local:http       Phatcharapons-Mac:50386 ESTABLISHED
tcp6       0      0 [::]:domain             [::]:*                  LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 localhost:ipp           [::]:*                  LISTEN
tcp6       0      0 [::]:3128               [::]:*                  LISTEN
tcp6       0      0 localhost:953           [::]:*                  LISTEN
udp        0      0 ubuntu.local:domain     *:*
udp        0      0 localhost:domain        *:*
udp        0      0 *:bootpc                *:*
udp        0      0 *:52430                 *:*
udp        0      0 *:mdns                  *:*
udp        0      0 *:40399                 *:*
udp6       0      0 [::]:domain             [::]:*
udp6       0      0 [::]:42126              [::]:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:42916              [::]:*
```

Picture showing the attacker's device's name

Q2

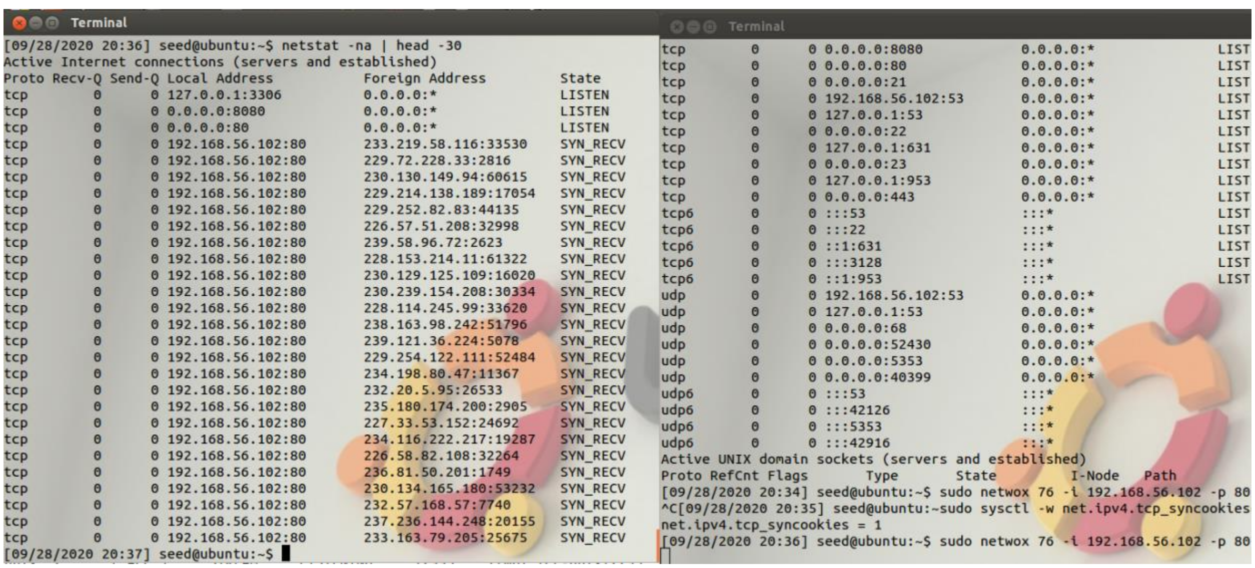
$ netwox 76 -i 192.168.56.102 -p 80



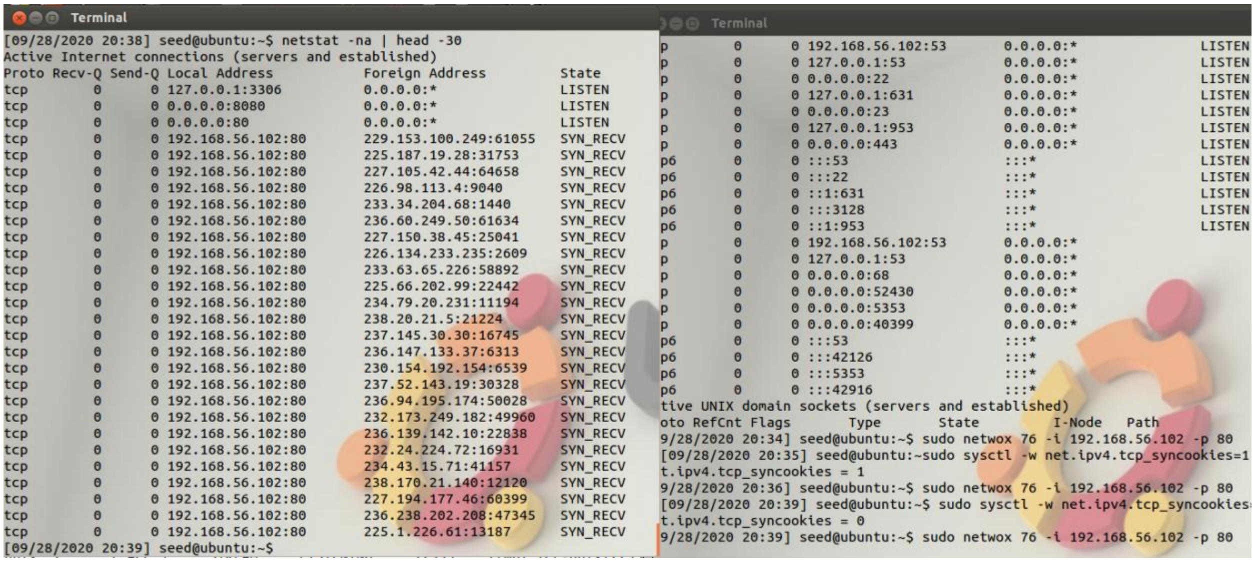
Running netwox command

Q3

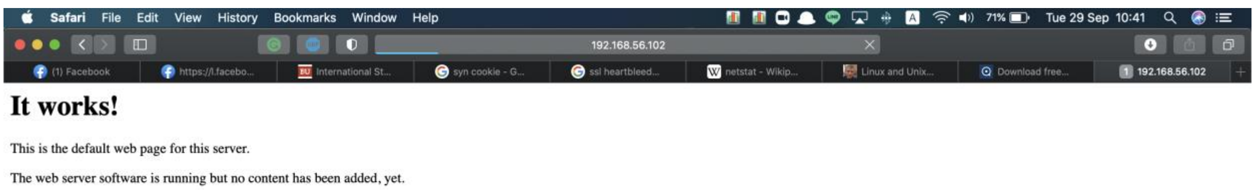
At first, with net.ipv4.tpc_syncookie=1, the browser can still connect 192.168.56.102.
But after turning syncookie to 0, the browser cannot connect to 192.168.56.102 anymore.



Running netwox command without turning syncookie=0



After turning syncookie=0



Notice that the browser is loading the webpage unendingly

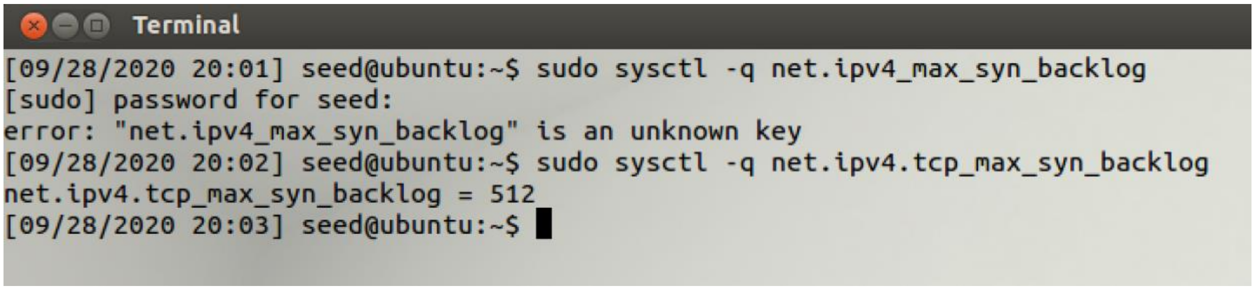
Q4

229.153.100.249
225.187.19.28
227.105.42.44

Q5

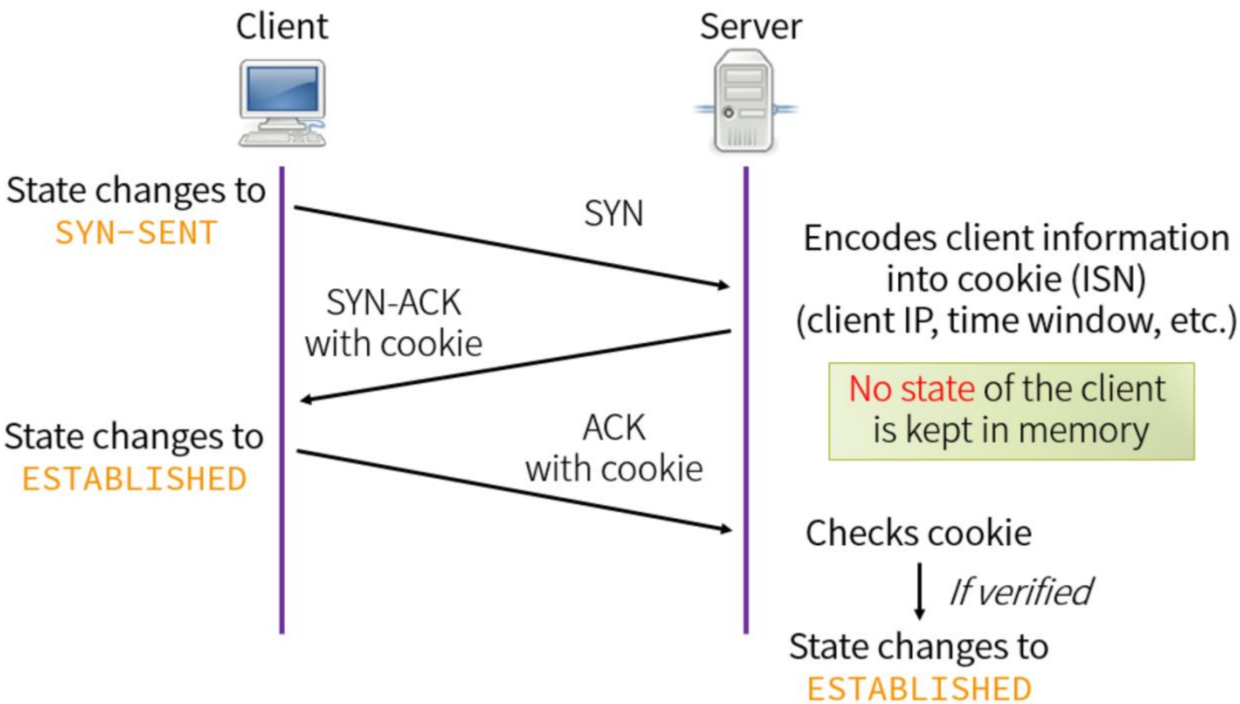
Net.ipv4.tcp_max_syn_backlog, as it is the maximum number of connection with the clients who did not acknowledge back to the server, once there are more than 512 dangling connections, the server is overloaded and stop responding.

So the number of resource is 512 connections, and all 512 was used in the attack which is the reason the server stopped responding.



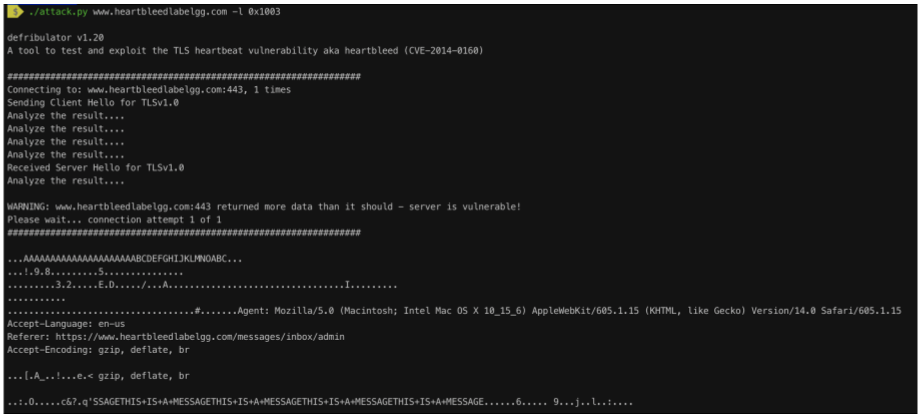
Q6

TCP SYN Cookie generates a sequence number using a secret mathematical formula that is quite impossible to guess, then put it in the SYN-ACK without allocating any memory yet. It will only allocate if the user reply with an ACK with a proper sequence number.

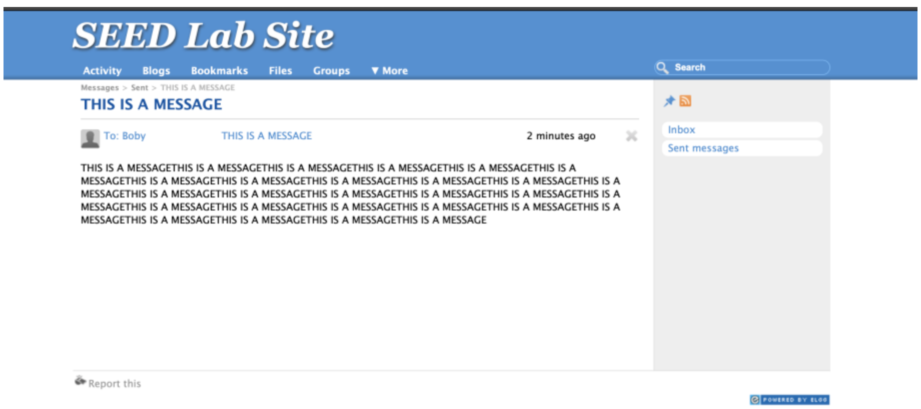


Source: http://kerugashi1981.changeip.com/Tcp-syn-cookies.html

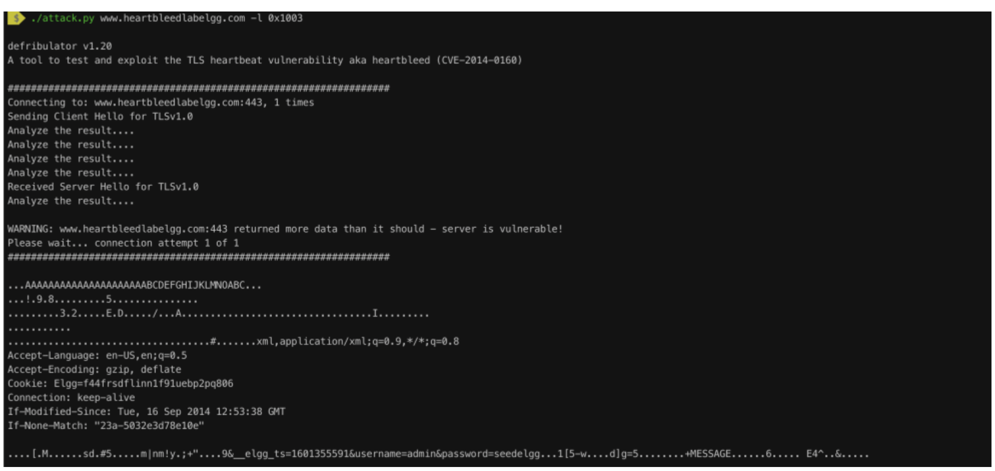
Q7



Picture showing secret obtaining from the server's memory through heartbleed attack



The actual message in the application



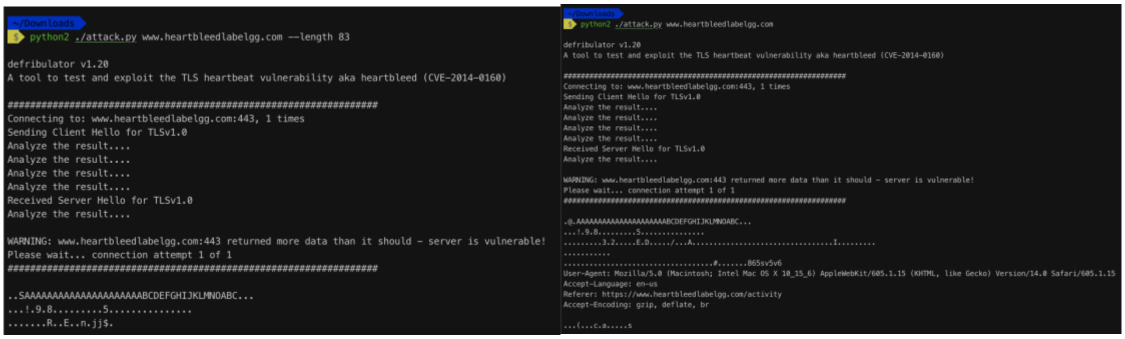
Picture showing username and password leaked from server's memory

Q8

With the attack.py program, I run it with multiple memory overflow length to scan for many possibilities of sensitive data. I manually run the program for a few times before I found the sensitive data which are the secret message, username, and password.

Q9

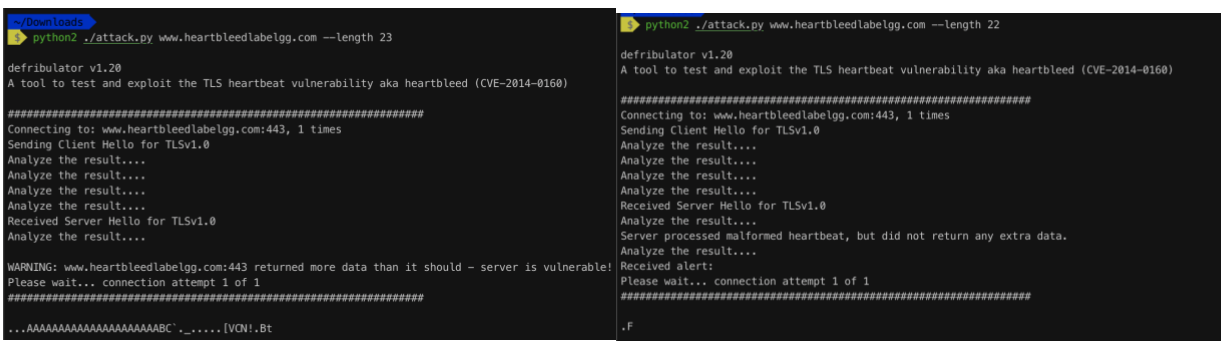
Smaller length variable yields in smaller payload obtaining from the attack.py program, as shown in the pictures below.



Smaller length variable on the left, and default length (0x4000) on the right

Q10

Length = 23 still yields the warning, while length = 22 stops showing the warning (stop returning any extra data)

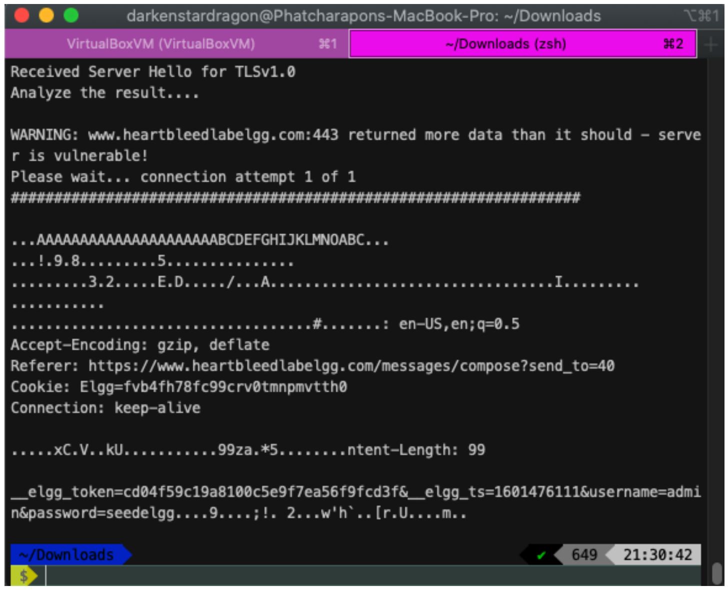


Length = 23, showing the vulnerability (left side) and length = 22 without any sign of vulnerability

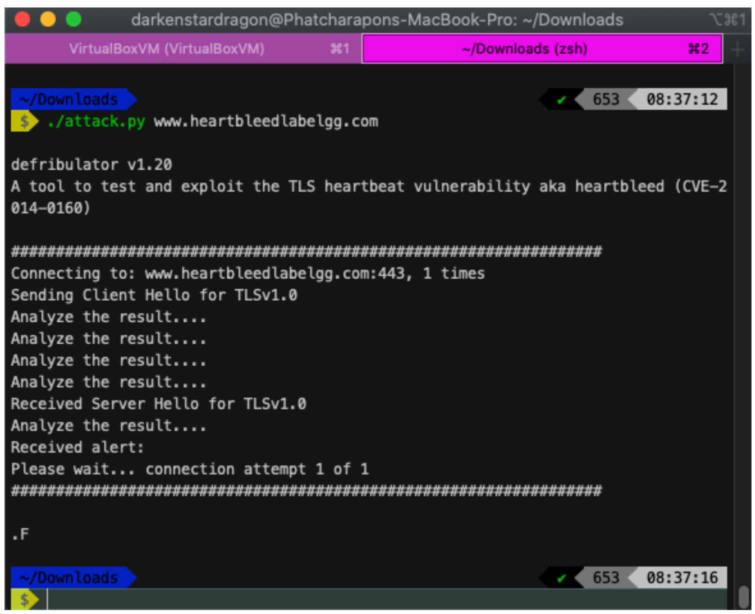
Q11

Not successful after upgrading the machine

Phatcharapon Jumruspun 6031040921



Before patching, still can get sensitive data from heartbleed attack



After patching, not leaking any sensitive data in the memory anymore

Q12

Server just needs to check if the variable payload_length actually is equal to the actual size of payload. Drop the packet if it doesn't. This way we can ensure that the response is going to be the same as the request, without leaking any sensitive data anymore.

Q13

Like proposed in the Q12, I think user input validation is always nice to have and would fix this vulnerability immediately, however fixing this is like fixing a vulnerability in frontend of the system, I believe we still have to fix the backend part which would be the boundary checking.

Reference for boundary checking fix (it is an official fix as well) :
https://github.com/openssl/openssl/commit/96db9023b881d7cd9f379b0c154650d6c108e9a3

```
26 ssl/d1_both.c
@@ -1459,26 +1459,36 @@ dtls1_process_heartbeat(SSL *s)
 	unsigned int payload;
 	unsigned int padding = 16; /* Use minimum padding */
 
-	/* Read type and payload length first */
-	hbtype = *p++;
-	n2s(p, payload);
-	pl = p;
-
 	if (s->msg_callback)
 		s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
 			&s->s3->rrec.data[0], s->s3->rrec.length,
 			s, s->msg_callback_arg);
 
+	/* Read type and payload length first */
+	if (1 + 2 + 16 > s->s3->rrec.length)
+		return 0; /* silently discard */
+	hbtype = *p++;
+	n2s(p, payload);
+	if (1 + 2 + payload + 16 > s->s3->rrec.length)
```

Example from the github commit for the heartbleed fix

While I think deleting the whole length to solve everything might not be practical as there would be no way to know which part is data and which part is padding anymore.